

Volume Forty-One, Number Three

DIGITAL EDITION Autumn 2024

2600

The Hacker Quarterly



Transitional Payphones



United States. Seen at the Missouri History Museum in St. Louis, we can't decide if this is their actual phone or part of a display. Perhaps every old payphone should be considered a museum piece moving forward?

Photo by Woody Krummenacher



Denmark. This classic model resides at a local hairdresser shop in Copenhagen after being obtained by a secondhand dealer. Note the pre-1993 Danish emergency number of "000" (now "112"). A much better fate than the junkyard.

Photo by Massimo Fiorentino



Japan. This elaborate setup is all part of Warner Brothers Studio in Tokyo and can be experienced as part of The Making of Harry Potter tour. An entire British phone booth of a bygone era is preserved here.

Photo by Maria Pursglove



United States. You can find this hip model on Biscayne Boulevard in Miami. We assume it no longer works, but even if it does, that's not what's important here. Every payphone can be beautiful, working or not. We just have to take the time to give them a makeover.

Photo by Cory Boehne

Got foreign payphone photos for us? Email them to payphones@2600.com. Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (more photos on inside back cover)

Listen

Turning Points	4
Further Password Discourse - Better Practices	6
Hacking the URL Schema	8
The Need for Hackers	10
What's Wrong With Us?	11
TELECOM INFORMER	13
Reverse Engineering: Tips and Tricks	15
To Be Cashierless or Not to Be Cashierless. That Is the Question.	17
Can ChromeOS Flex Actually Revive an Old Laptop?	18
The Burnout Machine	19
Introduction to the Robot Operating System (ROS)	20
Telecommunications Revolution	22
HACKER PERSPECTIVE	26
What Cops Really Want: Policing and Intelligence Gathering in the Digital Age	29
Modern Hackers as Collective Thinkers	31
Ten Teens and a Server Room	33
LETTERS	34
EFFECTING DIGITAL FREEDOM	46
Memories of a 30-Year-Old Non-coding Hacker	47
How Ubuntu Helped Me Escape a Cult	49
Reflections on Hacking and Teaching at State Universities	50
ARTIFICIAL INTERRUPTION	52
Journey of a Hacker: From Curiosity to Advocacy in Fairfax County	54
Keeping Hacker Culture Alive	58
Lee Williams, Harassment Agent Episode 3	58
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

Turning Points

2024 has been an historic year and will continue to lay the path for major changes ahead. None of us are unaffected by this.

Let's start with the good. We had our 15th conference this year and our second in our new home at St. John's University. For many, it was the first time we shared a "normal" gathering since 2018. COVID forced us to be virtual in 2020 and we were all compelled to wear masks in 2022. We also had a lot to learn in moving, not only to a new place, but to an entirely new part of New York City in the borough of Queens, proudly known as the most linguistically and ethnically diverse place in the *world*. That's a pretty big deal.

In the two years since A New HOPE, we managed to shape this year's version (HOPE XV) into something more worthy of a permanent setting. Our entire layout was changed. While the main building we used last time served us well, it didn't lend itself to a communal experience. That was actually better for when we were trying not to get too close to anyone, but we normally prefer rooms with lots of people rather than lots of rooms with fewer people. So we had three main gathering points this year, all close to each other, not requiring people to walk up a hill, and filled with great talks, workshops, demonstrations, vendors, and villages. St. John's gave us what the Hotel Pennsylvania never could: space. Attendees could mill about outdoors or inside, moving from one speaker track to another, never being in an uncomfortably crowded area nor in a place that seemed like a ghost town.

We addressed the issues of food options, bringing in food trucks and having more on-campus options provided by the university, as well as giving a much more detailed guide to the many places to visit off campus. Nearby hotels provided even more variety while on-campus housing added to the experience for attendees who wanted to be as close to the action as possible.

All of this is, of course, impossible.

That's what we were told by the experts; it's what we've always been told ever since we started having conferences. It's usually what any of us are told whenever we become determined to embark on a project that doesn't quite fit in with the norm. And considering the number of stories we heard told by our speakers of what they've been able to accomplish in the hacker world due to their determination and refusal to be swayed by all the naysayers, we believe HOPE is the right place to accomplish the impossible. We do that through determination, as well as the effort of a ton of volunteers and friends with access to the tools we need to conquer the technical challenges - from A/V to connectivity. We get there through attendees who believe in the mission to educate, inform, rebel, and share in a communal experience where inclusivity is a key ingredient. All of that serves to inspire us to keep going and to keep growing. We hope you feel the same way.

Moving on from the good to what may be the traumatic: this year is far from over, and when it is we will have experienced what could be the most historic election in living memory. We can't wait for it all to end.

Such events can teach you a lot about people, about our institutions, about ourselves. In the past however-long-this-has-been-going-on, we've learned a great deal about integrity, courage, cowardice, cult-like behavior, misinformation and disinformation, the dangers of social media, the importance of trusted sources, and *so much* about hypocrisy. When all is said and done, we have to move forward. Or destroy ourselves. Those are the only choices left at this point.

Disagreeing is a fundamental part of democracy. There is no progress without argument. But to shut someone down, to sever all links, to make them a non-person - it accomplishes nothing. In fact, it often fans the flames and drives people closer to

those who *do* accept them and listen to what they have to say, sometimes with increasing irrationality. We know it's not easy to put up with someone who has a warped view of reality or accepts as truth even the most egregious of lies. Difficult as it is however, disconnecting is a short term solution - and a self-defeating one. On November 8th, these people will still exist and they will likely still believe a good amount of what they've been espousing and regurgitating in recent years. So what then?

That's where the second choice comes in, the one where we destroy ourselves, a prospect more than a few have predicted. Some even appear to relish the idea. We don't. It's easy to give up, easier to light fires. We all have a base instinct hidden somewhere within us to lash out, attack, and employ violence. And maybe kicking it all to pieces and starting over again *is* the best way to get it right the next time. If it gets to that stage, then history will repeat itself once more. We're not convinced we're there yet.

It's good to be expressive, even to scream in frustration and anger on occasion. It can actually be really therapeutic. After expending that energy and releasing the bitterness and negativity, we're often ready to calm down and start over. And that's about where we've been as a nation recently. At some point, it has to get purged from our system, we have to start talking again, and we've got to live on common ground. We really hope that's the promise of 2025. We've had just about enough of the prelude.

An annoying update: this issue is coming to you about three weeks later than it should be. It took us years to make up all of the lost time caused by COVID and to get back on a normal publishing schedule. We finally got there with this year's Spring issue. It literally lasted only one issue. Our distributor wound up having some sort of communications snafu with their delivery people, resulting in *all* of our store-bound Summer issues sitting in a loading zone for the entire month of July, undoing all of that

work and costing us valuable shelf time all over the country. (Subscribers got the issue on time.)

While they regret the error, we are the ones who pay the price. That is how publishers are treated in this industry. This is far from the first time that we've been at the mercy of indifference and incompetence in the real world. Even digitally, companies like Amazon take more from us and give less every year, all the while putting any competition out of business. This is our unfortunate reality. It's why your independent support is so vital.

The upshot is that the next two issues will also be late (Winter by two weeks, Spring by one) until we once again catch up next summer. That is, assuming there are no more surprises.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2024. Annual subscription price \$31.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Issue Copies each issue during preceeding 12 months	Single nearest to filing date
A. Total Number of Copies		
B. Paid and/or Requested Circulation	19888	19550
1 Paid/Requested Outside-County Mail Subscriptions		
2 Paid In-County Subscriptions	5439	5428
3 Sales Through Dealers and carries, street vendors, and counter sales	0	0
4 Other Classes Mailed Through the USPS	12978	12695
C. Total Paid and/or Requested Circulation	0	0
D. Free Distribution by Mail and Outside the Mail	18417	18123
1 Outside-County		
2 In-County	131	127
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	0	0
E. Total free distribution	1184	1159
F. Total distribution	1315	1286
G. Copies not distributed	19732	19409
H. Total	156	141
I. Percent Paid	19888	19550
	93	93

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.

Further Password Discourse - Better Practices

by Modus Mundi

"I'm edumacated on every threat in the trade, Started checking the checker for any legerdemain" - Aesop Rock, "Legerdemain"

Hello again. At the end of my last article (41:1), I asked a bunch of annoying questions, and I'm sure it all felt like a setup - because it was! We'll run down some of the questions I put out there at the end of the article. Onward.

Should We Even Hash?

Something I didn't do in my first article was define what hashing is, or why we might hash over perceived alternatives. Real quick, when I talk about hashing, I am referring to the use of a cryptographic hash function (CHF) on a given string. NIST's definitions of a CHF¹ are interesting and generally all say the same thing.

Let's talk about alternatives. A few that stick out are:

1. Leave the string plaintext.
2. Obfuscate the string.
3. Encrypt the string.

To be clear - leaving a password in plaintext is a real bad idea. If an attacker breaches the system, they then have the plaintext representation of the password that they can then try on other systems. This terrible practice would permit credential stuffing attacks by default, which a security practitioner does not want to do. Obfuscation of the string, such as through some encoding mechanism, does little to dissuade an attacker. A smart attacker will determine the method of encoding and will ultimately decode - unless of course you're using the English alphabet only and ROT26¹, in which case you have ascended beyond this realm of minimally-crenulated bipeds and probably do not need this article.

Encryption, while tempting, is a path to madness. An unaware reader may be asking "Aren't they the same?" and to that I would make a grumpy face. Without going into a rabbit hole, the key difference between encryption and hashing is that encryption, given sufficient inputs, is reversible. This sort of reversibility is crucial for being able to archive sensitive data in a backup.

Having the capacity to reverse a given encrypted string sounds great, until we come to understand that the system that is doing this encryption and decryption must have the tools to do so available. Maybe this means the encryption parameters are local, backed by some HSM and the program we're utilizing is calling out to it, or maybe something completely different - there is a way to call back to the decrypter. A persistent,

skilled attacker can and will find that path to reversal and exploit it. As a builder of systems, consider what a reversible string really gets you before you do it. I advise you to generally avoid this. You might think to yourself "*I have a valid case,*" but please. Reconsider. It is likely that you can do what you need without a reversible string.

What Should We Even Hash With?

A problem with password hashing (also, a problem with life) is "what is best" depends on who you ask. If you're the U.S. government, you rely on the Federal Information Processing Standard, or FIPS. FIPS gets very specific about what can and cannot be used - and updates slowly, even if there have been significant advancements in the field that would give stronger passwords (or communications that are more resistant to attack). If you're in a different country, the government may have radically different cryptographic requirements (for instance, the Chinese government officially standardized SM3 for hashing passwords). I say this to point out that there will be many constraints depending on where you're standing, and if any of this applies to an actual business. If it doesn't, and it's just you out there in the wild, I would implore you to at least follow local laws around what can and cannot be used (if there are any). Don't be stupid with the law, folks.

There is a mountain of information out there about different hashing algorithms, and you as consumers of information should explore it. If you are not constrained by such things as government or industry requirements, there are smarter people than me offering guidance based on rigorous testing and analysis. For instance, from 2013 to 2015 there was a password hashing competition held that generally found Argon2 to be the best³. You may be thinking "It's been over ten years; hasn't something better come out?", and that is a valid question. This humble author is unsure; despite researching the topic for some time he has been unable to find an algorithm that is more widely regarded as "the most secure" or "better than" Argon2. This isn't to say it does not exist, but merely that I have not found it. It may still exist in the realm of crypto-wonk academia, which is beautiful and valid.

Should We Rotate Passwords?

Consider that your average user really hates change. They want a predictable experience and predictable outcomes. They also generally are going to be as low-effort about security initiatives

you put in place as they can be. So let's assume your organization has a password policy in place:

- At least eight characters
- One character must be an uppercase letter
- One character must be a lowercase letter
- One character must be a number
- One character must be a special character
- Password rotates every 60 days

The average user of this system will not be enthused, having to change their password every two months. Indeed, the particularly lazy may do something like the following to be compliant and maintain compliance with their passwords:

- Summer1!
- Summer2!
- Summer3!
- Summer4!

And so on. Your humble author can attest to seeing bad password practices such as this in the wild. On the other hand, we need to keep in mind that not forcing a user to reconsider their password can lead to compromise if they have used that password elsewhere. While I'm not here to tell you never to reset a password, I would offer that NIST's guidance per the 800-63 is pretty solid here; if someone may have gotten in, rotate it and rotate all of them ASAP. This guidance works for a vast majority of use cases and allows you to push password requirements comfortably.

All of that said... some environments may indeed be sufficiently high-impact that you need rotation (maybe even as short as 60 days!), but it is less likely. When in doubt, follow your industry/legal guidelines.

What Is Password Strength Anyway?

Without getting too insane, the "strength" of a password is a representation of how hard it is to determine through whatever cracking means is being used. A weaker password will be faster to crack than a stronger password. There have been a number⁵ of papers⁶ and implementations⁷ that go into this, and they need to be mentioned here so that you may stand on the shoulders of giants. To offer a short summary, password strength matters and is a combination of a bunch of factors. Research differs, but generally you want to ensure the password is at least one character class (this means alphabet characters, numerics, or special characters), at least 12 characters long, and has a password complexity that is estimated to require 10^{10} guesses. For instance, we might consider the string "modusmundi", which by using the aforementioned implementation⁷ we see has an estimated guesses_log10 of 8.57. The string "FrÃ¼hjahrsmÃ¼digkeit" scores an estimated guesses_log10 of 18. Perhaps this is because it is

not a dictionary term it has access to, but a smart attacker might. A perhaps easier-to-remember string of "capslockiscruisecontrolforcool" has a guesses_log10 of 20.00652. I say all of this to emphasize that length matters. Beating heuristics matters. Not much else seems to, from the research.

Thinking About Password Resets

There is a lot to get wrong with resetting passwords, and with account recovery in general. I'm not going to bore you too much, as there is a blistering amount of good information out there from people smarter than me⁸, but I will offer a few points I have experienced as a practitioner of the dark arts of identity. A trap that people get into when thinking about password resets is they want to be helpful. Do not be helpful. Do not let the attacker know if they are expecting a password. The response message for a successful password reset flow initiation should be the same as an unsuccessful password reset flow initiation; that is to say, something boring and along the lines of "If you're in our system, if you own the account you will receive more instructions." Reset flows should also take care to take the same exact time between a bad user request and a good user request. Reset flows should also take place as out-of-band as is possible, relying on a second factor of authentication where possible. (Some people are going to argue that an email is "something you have" and this works until a RAT is installed on the PC you bank and post cute cat pictures from). Reset flows should log people out immediately and everywhere if they have been successfully activated, and those same flows should notify the user it happened. I've seen what happens personally when these aren't implemented and, while there are other points, I feel like these aren't talked about enough.

While We Are Talking About Time...

As mentioned a moment ago, your password reset flow should take the same amount of time to fail as it does to succeed. The actual process of authenticating to a service is a whole different story. The hashing method used will drastically impact the speed by which a hash is generated and in turn will impact the time it takes to either crack a hash offline or have a server simply construct a hash of a given string. An MD5 hash, for instance, will be generated significantly faster than SHA512. Modern hashing methods, such as Argon2, offer the capability to change settings such that you can change the work factor. This means for a given piece of hardware, the CPU and memory usage of the hashing method can be tweaked to get certain time-oriented outcomes. There are no hard and fast rules here with respect

to tuning the hashing method. Instead we should understand that as we increase the time it takes to hash a given string that time cost is passed on to the service, and to the users. This can cause significant performance bottlenecks and service failures, all for the want of security! The Argon2 specs paper⁹ and IETF spec¹⁰ gives some food for thought, and OWASP¹¹ gives some good starting points. You'll see in a lot of modern service architectures people want to set Argon2 such that the hashing process takes anywhere from 250ms to a full second on the hardware they have provisioned to. This makes the parameterization important, as well as understanding the hardware being provisioned to.

With the rise of containerization, this becomes interesting, as 500 millicores of a CPU in 2025 will be nowhere near what 500 millicores will be in 2030, and individuals tuning these parameterized hashing functions will need to reassess their processes on a fairly regular basis. An astute reader might note that a problem we see with passwords is that the very math used to make them secure becomes trivial for future computing environments to, well, compute. This means responsible system owners are locked in a fairly steady arms race wherein they are moving to newer and better CHF's, updating systems to

maintain relevance in the face of new standards/requirements, and keeping abreast of what nefarious folks with too many GPUs on hand are able to do. This also means at least keeping an eye on such things as quantum computing and post-quantum cryptography, as at some point (perhaps soon) organizations will need to move to such systems and algorithms as simply the next stage of the arms race in securing systems.

Stay learning. Build better answers.

¹ csrc.nist.gov/glossary/term/cryptographic_hash_function

² rot26.org/

³ www.password-hashing.net/

⁴ pages.nist.gov/800-63-FAQ/#q-b05

⁵ users.ece.cmu.edu/~lbauer/papers/2012/oakland2012-guessing.pdf

⁶ dl.acm.org/doi/pdf/10.1145/3372297.3417882

⁷ github.com/dropbox/zxcvbn

⁸ cheatsheetseries.owasp.org/cheatsheets/Forgot_Password_Cheat_Sheet.html

⁹ www.password-hashing.net/argon2-specs.pdf

¹⁰ datatracker.ietf.org/doc/html/draft-irtf-cfrg-argon2-11#section-4

¹¹ cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Hacking the URL Schema

by **Tiago Epifânio (madcap)**

<https://madcap.pt>

Let's talk a little about the ancient art of generating URLs that look legit and similar to some address that you may know. There are several ways to do it.

The most common technique is called typosquatting and relies on the typos that we make when typing an address on the address bar. Like goggle.com or paypall.com. Although we get to those malicious sites by mistyping a website address, many people would also click on a link with that URL, not really noticing the typo.

There are also homograph attacks which rely on the fact that different characters can look very similar, like the capital I and the lower case L. Also there are different alphabets (Latin, Greek, Cyrillic) that have very similar symbols.

But in this article I'm going to focus on a different kind of attack called "URL Schema Obfuscation." It's so good that it allows you to create a fake URL that looks pretty normal and you don't even have to register a fake domain.

Let's say that you receive a legitimate looking link to a supposedly enraging tweet by some billionaire that you love to hate:

<http://twitter.com/elonmusk/status/@3264653699>

You click on it. But instead, you're taken somewhere else. In this case, you would be taken to the home page of *Phrack Magazine*.

How did this happen? Let's split the above address in parts and start by the end.

The 3264653699 part, which looks like the ID of a tweet, is indeed a disguised IP address in decimal format. This is a valid format, although most people don't know. An IP address is, in fact, a 32 bit number. It's easier to represent it in the normal dotted notation, separating it in four parts, each part having eight bits, like we usually do. But we can use it in decimal format as well.

Let's say that we want our victims to be redirected to the phrack.org website, which has the IP address 194.150.169.131. First, start by converting each part of that address into binary

format:

11000010.10010110.10101001.10000011

Remove the dots, obtaining a 32 bit value, and then convert it to a decimal number:

binary 110000101001011010101001100100011 = decimal 3264653699

Now, if you paste that decimal number into your browser's address bar, preceding it with http://, you will be taken to *Phrack's* website. Try it: <http://3264653699>.

But what about the rest of the URL (twitter.com/elonmusk/status/@)?

Well, this part also has some tricks in it.

First there's the at sign (@). That character, when placed before a domain name, means that you want to authenticate to that site using some username. Let's say you wanted to sign as user jaime at the site joana-blog.net. You would type <http://jaime@joana-blog.net>. This is not a very common means of authentication (nor a secure one), but it's a valid one. It was common in the old days to authenticate to FTP servers.

So, at the example given above, you would be authenticating at <http://3264653699> with the username "twitter.com/elonmusk/status".

Kind of. If you type that manually on your address bar, the browser will see those slashes and invalidate all that I've been saying. But instead of using regular forward slashes we can use a unicode character that looks like a slash but is instead interpreted as a regular character. In my example I'm using the unicode character U+2215 (division slash). You can see more details about it here: <https://codepoints.net/U+2215>.

So, after these small manipulations, you end up with a normal looking URL that will trick anyone because it looks like a valid address. That teaches us that we should be very careful when clicking random links even when they look legit (don't click links on suspicious emails, remember?).

Since this method only works when using http (instead of https), if you see a link that starts with "http://" you should probably avoid it. If in doubt, try typing the address manually into your browser.

Another thing you should do is use Firefox as your main browser. Firefox shows a warning saying that you're trying to login to a website that doesn't request authentication. Something like this:

Confirm

You are about to log in to the site '194.150.169.131' with the username 'twitter%2Ecom%E

2%88%95elonmusk%E2%88%95status' but the website does not require authentication. This may be an attempt to trick you.

Is '194.150.169.131' the site you want to visit?

(I wonder how many people will still click "OK" after this message anyway.)

Unfortunately, Google Chrome doesn't show that warning. And you know what? Seven out of ten people use Google Chrome or some variant of it, which makes an attack like this pretty efficient.

This is not a complicated method, but I created a Python script to make the creation of these URLs easier:

```
#!/bin/python3

import sys

URL_TEMPLATE = 'http://{ }@{ }'

if len(sys.argv) != 3:
    print('Usage: ./obfuscate_
↳url.py <fake_address> <real_
↳ip_address>\n' \
        'Example: ./obfuscate_
↳url.py twitter.com/elonmusk
↳194.150.169.131')
    exit(-1)

fake_addr = sys.argv[1]
real_ip_addr = sys.argv[2]

username_part = (
    fake_addr.replace('http://',
↳')
    .replace('https://', '')
    .replace('/', '\u2215')
)

ip_parts = real_ip_addr.
↳split('.')
binary_string = ''

for part in ip_parts:
    binary_string += '{0:b}'.
↳format(int(part))

print(URL_TEMPLATE.
↳format(username_part,
↳int(binary_string, 2)))
```

Be safe and beware of links with an at sign!

The Need for Hackers

by Eric Fassbender

I'm no hacker. I'm at the beginning of my journey, and I barely qualify as a script kiddie. However, what I am is an academic. One of the key problems for us academics is the timeliness of information. Due to the depth of research needed, the timeline of writing and approval of papers, and finally waiting for publication, academic analysis of current events tends to lag (at best) one to three years behind actual events. In the collective action and protest field where I work, many authors still draw their conclusions on the use of technology in protest from the Arab Spring in the early 2010s.

This presents us with a huge problem: in the last decade, the use of social media, the use of digital surveillance by nations, and the embeddedness of technology in our lives have changed drastically. Twitter, at the time a poster child of allowing disparate people to gather together and overthrow oppression, now spirals into endless controversies over censorship and social manipulation under a new name and leader. Other platforms also consolidate critical information on their operations behind algorithms protected by trade secret protections. This leaves academics at a standstill. The only information robust enough to draw conclusions from may be hopelessly out of date in relation to our society. This is a problem that hackers help solve.

Foregoing the Snowden leaks as a perfect example, a more recent case happened In 2020 when hackers obtained and leaked 269 gigs of data from U.S. law enforcement fusion centers in an event called BlueLeaks. This data, conveniently seeded by Distributed Denial of Secrets, is readily available for anyone with torrent and a few day's worth of time (my ISP is dreadful). This leak includes an amazing assortment of documents on U.S. surveillance activities and tactics, the scope of which is outside of this article but should be of interest to everyone. What is relevant, however, is that these kinds of leaks can give researchers decades back in their efforts to create timely and relevant work. There are several key ways that hackers provide a service to the academic community through leaking data.

First, and perhaps most important, leaked data allows research that would otherwise not be possible. Even if an academic had the technical skills and desire to hack an organization of

interest to them as part of a research project, they could never do so formally. In addition to the legal ramifications, academics are subject to the approval of institutional review boards for their research activities. If one attempted to circumvent these, they would be discovered in the review process, and their research would likely never be published. However, working with public datasets, illegal as it may have been for the initial hacker to obtain them, circumvents all of these issues. Review boards can approve the research, and academics can publish the work without fear of legal reprisal. It allows critical information to enter scientific debates, and inform new theories on state surveillance activities, social movements, and the impact of technology on society.

Second, leaked information is reliable in a way that public statements may never be. There is always the concern of public statements being edited and censored, as nations have incentives to misrepresent the extent and aims of their surveillance activities. Additionally, waiting to observe the outcomes of surveillance activities leaves the research at risk of being irrelevant, as tactics and targets may have changed by the time they are discovered. Additionally, the targets of surveillance and repression have already experienced negative outcomes. However, leaking internal documents solves both of these problems. The parties involved have no incentives to misrepresent the shared information; it is internal and not intended for public consumption. Additionally, while the actors involved are certain to change tactics as the leak occurs, they will be doing so without the added benefit of years of time, giving the subjects of their scrutiny time to adjust their tactics as well.

Finally, by lending their technical expertise, hackers help keep the public informed on the impacts of technology on society while those technologies remain relevant. As I stated before, knowing the full extent of the ability of organizers to utilize 2010s Twitter for starting mass movements tells us little about how today's X sides between organizers and the state. While the ivory tower by no means retains an unblemished reputation, academics are still given an amazing platform to inform and educate the public. Citizen science movements are growing, and community

outreach and education are rising as a priority for many research centers. Access to relevant information and timely information allows academics to use their privilege as educators to investigate the implications of leaked data, and work with community members to develop solutions in a way that few other institutions can. In addition to sharing information on state activities, they can also inspire interest in the skills that led to its discovery.

This information may come as no surprise to many of you. In fact, there may be no other audience available who is as well versed in the positive social benefits of hacking. However, this sentiment is not shared among as many

as it could be. Anti-state activities are heavily legislated, and many see them as both harmful and terrifying. The bridge between academic work and hackers serves as an avenue to highlight the social good that hackers play in our society. Elevating the discourse on technology and society shows that there are people capable of contending with the resources that nation-states and large companies wield and that they do so for the public interest. As one of those interested members of the public, I wanted to write this article to express that I'm thankful to the hackers out there who help me do my job better than I ever could otherwise. I look forward to seeing you more out here!

What's Wrong With Us?

by Ig0p89

People are leaving cybersecurity. This really isn't news to most of us. If they aren't leaving, the remainder of this segment are praying for death when they go to bed, so they don't have to endure another day dealing with egos, unrealistic deadlines, and the bosses. There are consistently large numbers of jobs open on the job boards and an individual company's website, as well as through recruiters calling and emailing at all hours. Annually, a new graphic is published showing the supply and demand curves with the difference growing larger every year, indicating the need for people is far outpacing the supply (that's you and me). To assist with the issue, there has been a push to automate as many processes as possible. While this may be beneficial in the long run, it is problematic for several reasons. These are symptoms of a larger systemic problem. What's causing this significant loss for the industry?

People Are Leaving Cybersecurity

We hear more and more about the skills gap. This is going to continue to grow as more technology is introduced and as the technology stack gains depth. All of this takes time, training, and resources to have the staff get up to speed with the technology. For example, if you are testing a new product using 5G and the company purchases the equipment for a cell station, not everyone will have the experience with this - setting it up or operating it. That takes time. Employers don't want to spend the money or employees' time with the training if they don't have to.

Too many times, people have posted astonishing job descriptions requiring mid-career experience for entry level pay. They may list the CISSP and years of experience for low analyst level pay. The HR department expects

the certifications, degrees, and certificates and also expects to pay as little as possible. The company's pay is not commensurate with their expectations. Just reading this drives certain people in the industry nuts as the lack of HR's grasp of reality kicks in.

Political Forces

This is always a favorite. Everyone wants to be the CISO. This is the paramount position for us. The power and prestige are an eternal draw for some. For nearly a year, I was in this role at a county municipality. I loved the work itself. I was helping secure the county's different networks, consulting with the court's admin to assist in guiding them. The network's configuration, tools, and most other aspects of IT were overly complex when they didn't need to be, and I was working to simplify this. While this was absolutely fulfilling, dealing with senior management (i.e., CIO, county board of commissioners, director of administration, et al.) made working there much more difficult than it needed to be. While there, my focus was doing the job. There was ample to do, and I worked late and weekends to get things moving forward. I kept my head down and did the work.

In short, the issue was that I well underestimated the power of politics. Even doing the right thing, following industry standards, and overtly using common sense will get you in trouble. For example, the sheriff's department requested a low-level manager to have complete unfettered access to everything and anything on the Internet. This manager was not out there on the streets trying to solve crimes, find child predators, or track down human traffickers, but was managing an out-of-the-way department that was completely

administrative and had no business having open access to the Internet or anything else. He really didn't like being told no to complete access to everything, so he complained to his manager, a captain, who then directed me to give him the complete access. The only reason given for this over-the-top access to anything on the Internet with absolutely no accountability was that he needed it for his job, which he obviously didn't. I put together a very clear document on why this was not a good idea for anyone and, if he needed access to a blocked website, I certainly would look at it right away. I let the captain know I couldn't do this due to the risks this would create. That did not go over well at all. Oh, and by the way, the county a couple of years before had a little issue with ransomware due to misconfigurations and click-happy users. This was a nationally published story and cost the county a lot, both directly and indirectly.

There was also an instance where a ticket came in requesting two laptops that was clumsily worded and did not attach any documentation that normally would have been required. This was also from the sheriff's department. The request was for two director-level county staff. The laptops were to only have Word and Excel with no access to any county resources, files, folders, etc. These would pretty much be set up as if you went to a big box store and purchased two laptops along with Microsoft licenses. There was also no documentation attached for the request. You know, if you don't get the paperwork prior to delivering the equipment, good luck getting it in a timely manner. As this was exceptionally odd, and I didn't want to get into yet more trouble with the sheriff's department - this time for treating these two persons differently than any other county employee - I asked questions.

Seemingly, if a ticket is not filled out correctly - or at all - and nothing is attached, you find out why and help the person complete the process correctly. There are policies and procedures in place for a reason. The requester refused to respond to any emails on why these two had to have such limited access to everything. The questions did not go over well, as you can imagine. It turns out the sheriff had a training plan/program in place for people incarcerated to teach them skills so when their sentence had been fulfilled, they could be gainfully employed, for example a plumber, electrician, or other job. These two somehow received enough training in this program while incarcerated to be director-level community event planners, even though they were felons

(two felonies each for murder and weapons charges) serving approximately 12 and 18 years. One of the two had applied for a job at the county and was turned down immediately. The sheriff had elected to override the hiring process.

The CIO was exceptionally irritated that I had followed protocol and asked questions to clarify the request. To this day when the sheriff talks to the board of commissioners, these two are standing behind him at the podium. The workers supported me, but senior management made it tough to be concerned with doing the right thing.

This was interesting, and I wrote a screenplay about it. Maybe you'll see more details of this on the big screen one day. However, I'll have the usual disclaimer of "This story is fictional. This does not depict any actual person, entity, or event [yada, yada, yada]."

I could talk about the sheriff's department's "bid" process for security, but this would be beating a dead horse. This added to my burnout, and lack of accountability by most levels of management was problematic. For these reasons and too many more (e.g., being told I did not smile as much as I needed to), I decided this was not the place for me. Also, if anyone thinks this couldn't have happened or I'm making any of this up, I have a complete set of notes for the timeline, notes from the ticketing system with dates and timestamps, meeting notes, etc. If nothing else, I'm thorough. One thing those newer to the industry need to appreciate is if you can't document it, it didn't happen. The printed materials I have will far outlive any of the senior managers' memories.

Loud=Correct?

In meetings, have you noticed the louder people are when discussing a topic, the more passionate they appear to be and the more correct? In multiple iterations, a manager may claim there are no tools to (fill in the blank). We accept what the manager says because they are passionate (but really just loud), even though a simple Google search finds four tools that do this and would work in the environment. When the manager is corrected, it doesn't matter. The damage is done. This wears down even the most dedicated, honest people.

In Closing

We need a healthy dose of reality and accountability. Unless some of the issues are resolved, this is only going to get worse. People may get upset with the changes; however, this is short-term and less costly than having staff leave due to burnout and idiocy. Something to think about.



TELECOM INFORMER



by TProphet

Hello, and greetings from the Central Office! For the longest time in recent memory, it was a relatively “normal” summer. The cedar trees around the Central Office aren’t dying from dehydration this year, and leaves are falling at the normal rate, at around the normal times. This means lots of big maple leaves, which litter the parking lot and the windshield of my car. Naturally, they stick like glue and have to be manually removed by yours truly in the pouring rain. But hey, that’s life in the Great Northwest.

On the way in the door today, I almost tripped over something I haven’t seen in awhile: a phone book. Yes, someone actually and un-ironically delivered a phone book to the phone company. In this area, a printed directory still exists, somehow, although it’s published by a small private local publisher rather than by my employer. This makes me realize that a lot of younger readers may have never seen a phone book outside of a museum, and also may have never made a call to directory assistance.

These days, if you need to find a product or service, your first stop is probably an Internet search engine (whether accessed on your computer or directly through your mobile phone). However, around the turn of the century (it feels so weird to stay that!), Internet searches were rudimentary. Even though it was the peak of the “dot com bubble,” only limited amounts of information were available online. If you needed to find a phone number, you’d look it up in the phone book or you’d call directory assistance.

When you subscribed to telephone service, by default on a 1FR, your name,

address, and phone number would appear in the next published White Pages. The White Pages contained (and in some cases still contain) residential and business listings, but not government listings which were included in the Blue Pages. Without paying for additional services, you were allowed to publish only your first initial and last name, and to only list the city of your address, but any more privacy than that required an additional “non-published” or “unlisted” service charge. What was the difference? If you opted for “unlisted” service (USOC NL), you wouldn’t be listed in the White Pages, but your number would still be available through directory assistance. If you opted for “non-published” service (USOC NP), you’d be kept out of both the phone book and directory assistance.

Business lines would get a listing in both the White Pages and the Yellow Pages, but phone companies made a lot of money with display advertising in the Yellow Pages, which was essential to get noticed in any sort of competitive category such as household services (plumbers, electricians, etc.). This was one of their primary sources of revenue, and it was over a \$20 billion business circa 2000 (by comparison, Google is currently estimated to make over \$150 billion in the U.S. annually). Surprisingly, directory publishing is (somehow) estimated to *still* be a billion dollar business! A lot of folks in their 60s and up still aren’t comfortable going online, and still use phone books.

Telephone directories are a hyper-local business, although there was occasional competition where independents operated. Directories typically covered a city or

municipal area. For example, in the Seattle area during the post AT&T breakup “US West” era, there were separate telephone directories for Seattle, Tacoma, Everett, and Bellevue-Eastside. However, GTE operated in the area; they published a Kirkland-Redmond-Bellevue directory which covered their territories. Businesses in the area tended to advertise in both the US West and GTE “Yellow Pages” so they could be found throughout their service area.

What if you didn’t have a phone book, or you wanted the phone number of someone whose number was unlisted (but *not* non-published)? And what if you needed a number that was out of your area, and for which you didn’t have the phone book? That’s where directory assistance came into play. The magic number was 555-1212; you’d call 1-555-1212 for your local directory assistance, and 1-NPA-555-1212 for long distance directory assistance. Local directory assistance was handled by your local phone company, and long distance directory assistance was typically provided by AT&T. In 1998, local directory assistance cost 60 cents per call (after one free call per month) in the US West service territory. Long distance directory assistance cost \$1.50 per call. AT&T also operated a toll-free directory assistance service at 1-800-555-1212, which provided toll-free numbers at no charge. However, businesses with toll-free numbers were charged to list their numbers in the toll-free directory.

In the early 2000s, voice services on mobile phones started to become inexpensive (with unlimited night and weekend minutes available on many plans), meaning people were making a lot more phone calls on the go - and a lot more phone calls from mobile phones in general. This meant a lot more directory assistance charges, because people rarely carried phone books around with them. Starting in the late 1990s and continuing into the early 2000s, the phone number

of directory assistance also changed to 411, which made calling even easier. Unfortunately, as a percentage, a lot more directory assistance calls failed to deliver because mobile phone numbers were all non-published. Also, from a mobile phone, directory assistance calls were all charged at the long distance rate (even for local numbers), and you had to pay whether or not they had the number you wanted. Making matters worse, phone companies got creative with directory assistance. They’d offer to connect you to the number after reading it rather than you having to hang up and dial it yourself, but this meant you were connected at a high, operator-handled rate!

All of the charges and shenanigans led to bill shock for consumers, and gave rise to services offering free ad-funded directory assistance. One such company, Jingle Networks, launched 1-800-FREE-411 in 2005 and, by 2008, had grown to handling approximately 20 million calls per month. The service wasn’t great, was driven by automated voice recognition technology, and it wasn’t particularly accurate, but it was free and this made it popular. Just as quickly as the business grew, though, it began to shrink. Around the same time, 3G data services and the iPhone launched. With the proliferation of more capable smartphones, search engines created online directories. These were overall pretty good and accurate, and a lot easier to use than a phone book. Consumers could look up numbers themselves on their smartphones rather than having a directory service operator do it for them.

And that leads us to the world of today. I’m not sure what to do with this third-party telephone directory, full of questionable business listings, which was crudely printed offshore on low quality paper. Maybe I’ll look in the landscaping category and see whether someone there can handle all of these leaves. In the meantime, enjoy your autumn, drive carefully, and I’ll see you in the winter!

Reverse Engineering: Tips and Tricks

by Nikolaos Tsapakis

When reverse engineering, time spent is very important. Especially in our days where people are more and more occupied and busy. In this small guide, I will provide some tips that may accelerate this process and mature your skills. Let us now begin.

Functions

It is very common for coders to write a function in order to perform a specific task and then reuse it. In many cases, such a function would return just a success flag and code will validate the outcome based on that flag. Modify that flag and you may be able to switch from “bad boy” into “good boy.” In most cases, that flag would reside in EAX/RAX after the function exits. But in other circumstances, a function may not only return a flag but also an object. Such an object can be in the form of a structure in memory with a valid pointer. If you try to modify the return value, that would most probably result in application crash due to memory access violation, since it would try to still use a non-existing object. In such a case, emulation is a possibility. That would mean trying to craft function return data which are similar to the expected object and its structures. In such a case, you would need to understand that function in order to emulate its behavior.

AntiDebugs

Check the application behavior running under debugger versus not running under debugger. If the application terminates unexpectedly under debugger, then debug tools have probably been detected. There are so many anti-debug tricks which can be used to prevent debugging and reverse engineering. Some of them detect the modifications a debugger performs on the process when being debugged. Those modifications may include larger execution time between different parts of code (since a debugger pauses in between), changes in internal process structures (like the BeingDebugged flag in the PEB), changes in machine environment (like the presence of processes related to debug tools), environment checks (like running on a virtual machine (VM)) and much more. The best approach against these checks would initially be to use ready-made plugins which disable anti-debug mechanisms in a massive way. An example of such plugins could be x64dbg anti-anti-debug plugins⁰¹. You can go through the list of anti-anti debugs in the plugins and look for more information using search engines. If

you still suspect that application detects the debugger then you should go step by step and trace up to the part of code which changes its flow to process termination or other unusual code exits.

0xEBFE

The 0xEBFE trick is a two byte sequence which is assembled into JMP EIP. That would mean the program will execute that instruction and indefinitely pause its execution (self jump). It is a nice trick in order to make the program stop where you wish without the need for attaching a debugger from the beginning of the application execution. The trick would be the ability to bypass some anti-debugging detections. For example, any code that would run prior to self jump instruction would not detect debugging since it makes sense to attach the debugger after the application executes the self jump instruction and pauses in memory.

File Tampering

Avoid modifying the file and try modifying memory only. For example, you may write a program (which is called a loader) which runs the application and then injects code in memory depending on the program manipulation you wish to achieve. The reason for that is you may bypass file tampering detections. File tampering can be detected using various methods like checksums and digital signature checking. Python is a great language for writing such a loader⁰². Moreover, there may be other tools which can generate loaders based on execution conditions and input. One such example is the following reference⁰³.

Automation and Plugins

Try using existing plugins⁰¹ for your reverse engineering actions. For example, if you are using x64dbg, then try using supported plugins which bypass anti-debugs or perform other actions like dumping memory regions or fixing imports. By studying the plugins and their code or configuration, you may learn lots of things for their functionality and use this knowledge for your future quests. Try to automate stuff by using any tool your debugger provides. Most debuggers have scripting capabilities to interact with the debugged application. Discover and try using those capabilities.

Online Versus Offline

Find out how an application behaves when being online versus being offline. In general, it is always a good idea to notice high level

application behavior before going deeper into assembly code. That could save much time that would result in going through tons of code, probably wasting lots of energy and time for nothing.

Recon

Try accumulating public information for older version(s) of the same application. Such research could reveal interesting high-level functions and is a must to know before going deeper into assembly code. Application evolution may also reveal interesting information on how certain functions evolved and got more complicated through time. Places such as developer forums, vendor sites, Github repos, or personal accounts may be a gold mine in regards to the application history and evolution.

Testing Environment

Make sure you have a dedicated environment for conducting your experiments. Setting up virtual machines like VirtualBox⁰⁴ would be ideal in order to take snapshots for tracing and restoring the snapshots if tracing was not successful. That will save much time to reach a debug point. You may create many different environments like a snapshot with no debugging tools at all (fresh) and another with debugging tools. You may try to run the application on fresh versus non-fresh snapshots and notice differences in behavior. Make sure you have all necessary tools like IDA dasm⁰⁵, x64dbg debugger⁰⁶, process explorer⁰⁷, process monitor⁰⁸, a hex editor, and an API monitor⁰⁹. Keep in mind that applications may behave differently when running under a virtual machine. For example, some apps may detect running inside a VM and abnormally terminate. Applications like games may also not run correctly in a VM since proper 3D capabilities may not be available.

Security Products

In regards to the testing environment, having a network connection and a security product installed (like an antivirus) on the test machine could be a challenge depending on the type of research. Security products may leak lots of information about your research. They could send out telemetry related to filesystems, registry, running processes, network connections, and more. Perhaps it is optimal to do all research and

testing on a clean machine except if research does not mandate such a need.

High Level Process Info

Before going deeper into your analysis, try to find out as much high level information for your running application as possible. For example, you may check for open handles, remote communication hosts, command line input arguments, parent and children processes, process environment variables, loaded modules, and much more. Try to spend some time interacting with the application and observe changes in its behavior. That would generate important knowledge which you can use it in the next steps of your analysis.

Debug Mode

A couple of important traits that may assist your analysis are strings and debug messages. It may be possible that you would execute the application in some sort of debug mode which could dump logs with valuable information. Logs may be dumped into a file or on the debugger itself. Always check public available information and binary/memory strings in order to discover input options that would allow the application to run in development or debug mode.

Last Words

I hope this short guide provides you with some helpful information in order to increase your analytical skills. But the most important properties for you to have throughout the journey are curiosity and imagination. Good luck!

References

⁰¹github.com/x64dbg/x64dbg/wiki/Plugins

⁰²www.youtube.com/watch?v=fv1kgdngGlQ

⁰³github.com/anomous/diablo2oo2-s-Universal-Patcher-dUP-Windows

⁰⁴www.virtualbox.org

⁰⁵hex-rays.com/ida-free

⁰⁶x64dbg.com

⁰⁷learn.microsoft.com/en-us/sysinternals/downloads/process-explorer

⁰⁸learn.microsoft.com/en-us/sysinternals/downloads/procmon

⁰⁹www.rohitab.com/apimonitor

PDF & EBOOK SUBSCRIPTIONS!

Yes, we finally did it! You can now get a PDF subscription or have issues in EPUB3 format for Kindles and other ebook readers. No DRM or any sort of copy restriction! Subscriptions range from one year to lifetime in the format of your choice.

Just visit the SUBSCRIPTION section at 2600.store

PLEASE HELP US SPREAD THE WORD

To Be Cashierless or Not to Be Cashierless. That Is the Question.

by blue_elk934

Last month I read a news story on the Internet about a new technology introduced in Italy: the cashierless store.

In that moment, my half nerd's heart said: "Incredible, the supermarket is becoming like *Star Trek*. I must try it." But two seconds ago, my half security's heart said: "Damn it, surely cybersecurity issues will come up."

Before I go into my concerns over security, I want to explain what a cashierless store is and what technology is used.

A cashierless store is a store which allows customers to shop for their products and leave without having to wait in queue and pay at a checkout.

The process of shopping in a cashierless store can be broken down into four phases:

- **Before-purchase.** An app may need to be downloaded.
- **Check-in.** A bar code from the store's app may need to be scanned in order to enter the store.
- **Product selection.** Products can usually be selected without taking any previous actions, but some stores require customers to scan a bar code on the product or tap a screen to select products.
- **Check-out.** Stores utilize sensor fusion and deep learning for computer vision to allow customers to walk out with their products without waiting in line at a register.

To realize the four phases, there are two necessary and important bits of technology:

1) **Sensor fusion** marks each customer with defining features and uses cameras and pressure sensors together to keep track of where each customer goes and what they take from the shelves. Sensor fusion has two "advantages:"

- It gathers information from different sensors and compiles it to create an accurate representation of what is happening and the relative positions of objects in an area at a specific time.
- It's often more accurate than single sensors since the separate measurements can be used to double-check and narrow the margin of error.

2) **Deep learning for computer vision** is used to track customers and products using:

- **Object detection.** This is the process of identifying objects within an image. Object detection is useful in identifying instances when a customer picks up and puts down an

object, or for identifying the products on each of the shelves.

- **Multi-target tracking.** What this does is approximately locate a moving person within consecutive frames of images. Multi-target tracking allows stores to keep track of each customer and their actions, like what products they picked up and put back and when they entered and exited the store.
- **Pose estimation.** This is the process of using an image to track a person using the positions of their body parts, like their head, hands, and wrists. Similar to multi-target tracking, pose estimation allows stores to keep track of customers, providing information for the computer to determine which customer interacted with the store, like when a product is grabbed.

With this detailed explanation of the technology, let's move on to the advantages and disadvantages in the "human" sphere that we surely know or that we have heard:

- No queue at the checkout.
- These stores are always open 365 days a year.
- Because they are small stores, this is mainly suitable for buying very few things and not for weekly shopping.
- Only cashless payments for the checkout are accepted, thus preventing the tills from always having the "correct change" and from possible robberies by thieves.
- Building the structure of a cashierless store is very expensive.
- For older people, it is not easy to approach this technology.
- There is no cashier at the till, so the human touch is missed.

Let us now discuss the cybersecurity issues to consider:

1) **Data profiling** by stores towards users by making targeted advertisements, etc., based on purchases made.

2) **Using cameras** to frame customers' faces at the entrance to prevent identity theft and to avoid customers having to always scan its QR code ID (example: Amazon GO).

3) The technologies used evolve often and the **risk of cyber attacks** by malicious people is very high because these systems are always on 365 days a year.

For these described points, there are some solutions:

- 1) The stores should explicitly ask if the

customer wants targeted advertisements based on purchases made.

2) Honestly, I am not aware of any debates in the U.S. for Amazon GO, but in the European Union they are trying to ban facial framing for GDPR reasons and replace it with only QR code ID, but a question arises for me: if the store does not use facial recognition and someone steals my smartphone, will the thief do the shopping for free?

In my opinion, the best solution would be to adopt biometrics (e.g., fingerprint in Android systems or Face ID for Apple systems) to “unlock” the QR code because biometrics allows the customer to be uniquely identified.

Obviously, the biometric data should remain in the customer’s smartphone and not shared with the store - otherwise privacy will go out the window!

3) A plan should be established to update the technologies used and monthly penetration

testing plans should be implemented to avoid possible cyber attacks from malicious people.

Here we come to the conclusion: we have talked about the technologies used to make these cashierless systems, their advantages, disadvantages, and cybersecurity concerns.

I don’t like to conclude with apocalyptic or negative phrases, but I would like to end the article with this question that should give us pause for thought:

Would you skip the checkout queue to gain time by giving up the privacy we all desire (but magically forget when convenience presents itself) or, if you are truly a “guardian” of privacy, would you wait patiently for your turn in the queue?

Hoping for an answer to this question, I would like to thank everyone who made it to the end of the reading and the editorial staff for publishing my article. See you next time!

Can ChromeOS Flex Actually Revive an Old Laptop?

by Acidity [aka ItsT3K]

Recently I picked up two old Thinkpads at a hamfest with the intent to re-purpose them as little Linux laptops. And, as a definitely sane and normal person, I decided to throw ChromeOS Flex on one of them. One of the things that led me to do this was the fact that you can now run Linux applications on it. This seemed very promising.

First off, I won’t bullshit. Linux on ChromeOS isn’t the Linux base of the OS, which disappoints me. Rather, it’s just a thin VM that runs Debian Linux inside ChromeOS. This means that if it runs on Debian, it should run on ChromeOS... *riiiiiight?* Presumably yes, and as all of the programs I usually use seem to run perfectly fine, I mean hell, I’m writing this very article in LibreOffice running on that very ChromeOS Flex install.

But this would not be a 2600 article without some complaining! So first off, here are the bad things:

- It requires a Google account - which is obvious as it’s ChromeOS. But it makes it even worse that you cannot use the Linux Development Environment in guest mode. Meaning the Google account is mandatory!
- Graphics are a hit and miss - more graphically

intensive websites under Firefox ESR were laggy at best and slideshow speeds at worse. GIMP, on the other hand, was a bit more usable. Though graphical effects (namely distortion based ones) were sluggish, they still rendered in the image just fine. (Note: as I’m typing this I’m noticing a few slight graphical bugs with my cursor, but this could just be the old graphics chip.)

- Performance takes a hit - this is to be expected, it’s a virtual machine for damn sake. But I decided to benchmark the one thing ChromeOS is good at, web browsing! And using Speedometer 3.0 (browserbench.org/Speedometer3.0/), I got to see how much of a hit performance took.

Firefox ESR under Linux on ChromeOS: 1.94 / 140
Chrome under ChromeOS on ChromeOS Flex: 5.33 / 140

It was a notable hit too.

Anyways, enough bitching. Can it revive an old laptop like Google claims it will? Kinda yeah, it makes it a lot more usable than Windows ever would. But it’s no more usable on this Thinkpad X230 Tablet than Debian itself would be.

WRITERS NEEDED!

Send your articles on hacking & technology
to articles@2600.com

The Burnout Machine

by Bioszombie

Let's get real for a minute: the tech industry loves to sell us on the myth of the "dream job." You know the pitch - beanbags in the office, free kombucha on tap, and "Agile" processes that are supposed to make everything more flexible, more efficient. But the reality? It's a meat grinder that chews up developers, sysadmins, and infosec pros and spits them out the other side - burnt out, disillusioned, and disposable.

We're living in a world where billion dollar tech companies expect us to live and breathe code, demanding 80 hour weeks under the guise of "passion." And what do we get in return? Burnout, anxiety, and the constant threat of layoffs. It's time to face facts: this industry isn't your friend. It's a machine, and unless we start organizing, it's going to keep grinding us down. It's time to talk about unionizing tech jobs.

Remember when Agile was supposed to save us all? Flexible sprints, self-organizing teams - yeah, right. In practice, Agile has been twisted into a tool for management to push us harder and faster. They say it's about "responding to change over following a plan," but let's be honest - it's about doing more with less and keeping us on a treadmill that never stops. The sprint becomes a marathon, and we're the ones paying the price.

And then there's the burnout. We're in an industry where burnout isn't just common - it's expected. If you're not pulling all-nighters, you're not "committed." If you're not answering Slack messages at midnight, you're "not a team player." This culture is toxic, and it's only getting worse. The relentless churn of projects, the constant pressure to innovate, and the ever-present threat of obsolescence create a perfect storm of stress. And what's the industry's solution? A mindfulness app and a lecture on work-life balance. Give me a break.

Let's talk about job security - because there isn't any. The tech industry loves to hype itself as a meritocracy, where the best and the brightest rise to the top. But in reality, it's a meat market. As soon as you're not "on the cutting edge," you're out. Outsourcing, contract work, gig economy bullshit - it's all designed to keep us insecure, to keep us grinding away at the next big thing with no guarantee that we'll have a job next week, next month, or next year.

Companies love to brag about their innovation, but the real innovation is finding new ways to make us disposable. Permanent employment? That's for suckers. Why pay benefits and offer

job security when they can churn through contractors and freelancers like cheap code? And don't get me started on those non-compete clauses - designed to keep you locked down and terrified to make a move that might actually be good for your career.

And let's not forget the ethical side of this equation. We're being asked to build the future, to develop AI, blockchain, and all the other buzzword technologies that are supposed to change the world. But at what cost? How many of us have been forced to work on projects that make us sick to our stomachs - surveillance tech, data mining tools, algorithms that reinforce societal biases - because we don't have the power to say no?

That's the kicker. We're the ones building the damn future, but we have no say in how it's built. We don't get to decide whether our code is used for good or for evil. And as long as we're isolated, as long as we're afraid to speak out because we might lose our jobs, nothing will change.

This industry isn't going to fix itself. The billionaires at the top aren't going to suddenly grow a conscience and start treating us like humans. They'll keep pushing, and we'll keep breaking - unless we organize, unless we unionize.

Unionizing isn't just about getting better pay or benefits (though we desperately need both). It's about taking back some control. It's about having a say in how we work, what we work on, and how we're treated. It's about saying no to the endless churn, the burnout culture, the gig economy bullshit.

And don't let anyone tell you it's impossible. The Alphabet Workers Union at Google? They're showing us it can be done. They're standing up to one of the biggest companies in the world and saying, "Enough." We need more of that. We need to take that energy and spread it across the industry - across all the companies that are profiting off our sweat and tears.

Hackers, we've always been about more than just code. We've been about freedom - freedom of information, freedom from control. Unionizing is the next logical step. It's about taking the hacker ethos into the workplace, about organizing to protect ourselves and each other.

- *Start the Conversation:* Talk to your coworkers. Break the silence. The first step to

organizing is realizing you're not alone.

- *Support Existing Efforts:* If you're in a company where union efforts are already underway, get involved. If not, start thinking about how you can start one.
- *Use Your Skills:* We're hackers - we know how to communicate securely, how to organize without being detected. Let's use those skills to build something real, something that can stand up to the powers that be.
- *Push for Ethics:* Let's make sure that any union platform we build isn't just about wages and hours, but about ethics too. We need to have a say in what we're building and how it's used.

The tech industry is a runaway train, and if we don't do something soon, we're going to get run over. The burnout, the job insecurity, the ethical nightmares - it's all going to keep getting worse unless we take a stand. Unionizing isn't just a nice idea - it's a necessity.

So let's do what hackers do best: let's disrupt. Let's take the tools they've given us, the skills we've honed, and use them to build something better. Let's unionize. Let's take back our industry, take back our jobs, and take back our futures.

The future of tech is being written right now, and it's up to us to decide what kind of story it will be. Let's make it a story we can be proud of.

Introduction to the Robot Operating System (ROS)

by Gazza

It has been a minute since I submitted an article and for that I apologize. For reference, my last submission was published in Volume Thirty-Four, Number Four. I was inspired to write this after reading about Amazon's Astro robot.¹ In short, with my interest in robotics, I wanted to see how many of Astro's features I could replicate with open source software on my new Create 3 robot.²

Personally, I have been working in the field of robotics since 2016. I work mainly with the Robot Operating System (ROS).³ ROS had its start with a company called Willow Garage back in 2010. Now ROS is managed under the Open Source Robotics Foundation (OSRF).⁴ The ROS releases are typically tied to a specific Ubuntu distribution and are alphabetical in nature. Thus, when I started playing with ROS in 2016, I was using the Kinetic Kame, which ran on Ubuntu 16.04 (Xenial). Note the OS portion of ROS is a bit of a misnomer, if you are a Linux distro hopper like myself. ROS is more akin to a Linux package than an OS. Presently, the latest (and last) release of ROS 1 is called Noetic Ninjemys and is supported until May of 2025. Noetic runs on Ubuntu 20.04 (Focal) release. It can also be installed on Debian. Windows 10 and Arch installations are marked as experimental. Note that ROS 2 Ardent Apalone, a complete rewrite of ROS 1, was released in 2018. Presently, at the time of writing there are three ROS 2 releases: Rolling Ridley which, as its name implies, is a rolling release, Iron Irwini which has an EOL of November 2024, and Humble Hawksbill which has an EOL of May 2027. The newest Jazzy release will be out when this article publishes. Note ROS releases typically alternate between an LTS version and an updated version similar to the Ubuntu cycle. As a personal preference, I typically stick to the LTS releases. Also, I am

currently making the switch to ROS 2, so I feel more comfortable to continue focusing on ROS 1 for this article.

My very first robot was a Turtlebot 2, think roomba, equipped with a Kinect for Xbox 360. I make the distinction between Kinect for Xbox 360 and Kinect for Xbox One because they used different technologies. The 360 version used structured light. In short, structured light projects a bunch of dots in a specific pattern. Deviations in the pattern is how the Kinect detects the user and calculates how far away they are from the camera. The typical range of a Kinect sensor is six to eight meters. Note that the Xbox One version used time of flight to detect the user. I chose the Kinect since you could pick one up for around 200 USD. While a 360 degree 3D LiDAR would be a better choice, in 2016 the cost of a Velodyne VLP-16 was well over 10k USD (presently you can pick up a 16 beam 3D LiDAR for around 3.5k USD). Also for reference, a 360 degree 2D LiDAR is now around 300 USD.

On the Turtlebot 2, I used the Kinect for obstacle avoidance as well as to map the environment; more on that later. Note the structured light version of the Kinect would not work outdoors, but the time of flight version did a better job in sunlight. On my new Create 3 robot, I use either Intel Realsense D435s or an Oak-D camera from Luxonis.

Presently, I am primarily interested in navigation and autonomy so that is the first of Astro's features I would like to replicate. There are many different levels of autonomy from Level 1, think of a remote controlled car, to Level 8, what you see in movies. These levels are based on a paper published by Bostelman and Messina.⁵

Let's start with Level 1. In ROS, you can use the packages "teleop_twist_keyboard"⁶ or "teleop_twist_joy"⁷ to drive the robot around

with either a keyboard or joystick respectively. Both of these packages publish the topic “cmd_vel”. At its core ROS is a messaging system that subscribes and publishes messages. In this case the “cmd_vel” topic is what gets the robot to move. Note however with “teleop_twist_keyboard” or “teleop_twist_joy” the robot will behave like a remote controlled car and run into things if you’re not careful. Now to get to an autonomous level of 6, we need to use a ROS package called “move_base”.⁸ The “move_base” package subscribes to a “move_base_simple/goal” topic and publishes a “cmd_vel” topic. How do we generate a “move_base_simple/goal” topic? In short, we use a package called RViz that allows you to visualize ROS topics in a 3D environment.⁹ For our intended use case RViz has a button called “2D Nav Goal” which we can use to set a way point or “move_base_simple/goal” topic on a map. Where does the map come from? One way is to use Simultaneous Localization And Mapping (SLAM) to create one as you explore.

Making a map is the second of Astro’s features I want to replicate. Note these maps are typically 2D and have three values; specifically “NO_INFORMATION”, “FREE_SPACE”, and “LETHAL_OBSTACLE”. A common SLAM package is “gmapping”.¹⁰ The “gmapping” package subscribes to a “scan” topic and uses the data to publish a “map” topic. The “move_base” package can also subscribe to this “map” topic and makes two cost maps, specifically a “global_costmap” that is typically static, and a rolling “local_costmap” that moves with the robot. Thus when you drop a way point with the “2D Nav Goal” in Rviz, “move_base” uses a “global_planner” (the default is NavfnROS) on the “global_costmap” to plan a path for the robot to reach the way point. Simultaneously, “move_base” also uses the “local_costmap” and a “local_planner” (the default is TrajectoryPlannerROS) to avoid any obstacles encountered along the “global_path”. Obstacles are detected in the “Obstacle_layer” of “move_base” and typically uses either “LaserScan” or “PointCloud2” messages to identify obstacles. Note the Kinect, D435, and Oak-D are all capable of generating a “PointCloud2” topic. The “move_base” package also has an “inflation_layer” that can be used to add additional padding to the map or obstacles the sensors identify to keep the robot from running into things.

Setting way points is typically how I operate the robot, but we can take it a step further. We can also let the robot explore on its own using “explore_lite”¹¹ getting us to Level 7. The “explore_lite” package uses frontiers to set its own way points. A frontier is defined as the

boundary between “NO_INFORMATION” and “FREE_SPACE” on the occupancy grid. The longer the frontier the higher the priority and continues until all frontiers are cleared.

The ability to patrol is another of Astro’s features I want to replicate. We could do this with a series of way points, but I would have to ensure that the way points were clear of obstacles at all times. The advantage of using “explore_lite” over way points for patrolling is I can move my furniture whenever and wherever I want. If you want your robot to auto dock when it’s low on battery, then we can use a ROS package called “apriltag_ros”.¹² The assumption is we have an AprilTag on the docking station. If we want to have the robot recognize objects, then we could use the ROS package “find_2D_object”.¹³ However, we would need a picture of the object the robot is looking for. Note that there are definitely more robust approaches to object recognition such as YOLO that may be a better fit for your use case.

Astro has quite a few other features that look really interesting, like a camera on a periscope, but I think that is a good start for now and I should probably wrap up this article. Stay tuned for my next submission, already in progress, on how to set up a simulated robot in ROS with most of the aforementioned packages. As I finish this, I am now getting, “Have you seen this???” messages from coworkers and friends in regard to a flame throwing robotic quadruped. Specifically, the Terminator from a company called Throwflame.¹⁴ The price tag, at the time of writing, is just under 10k USD. Note that the ARC flamethrower can be purchased separately for under 1k USD. Now I am thinking of how could I mount one to my Create 3. If I did, it would definitely need a catchy name like Thermoroomba or Thermoomba.

¹www.aboutamazon.com/news/devices/amazon-astro-2022

²edu.irobot.com/what-we-offer/create3

³www.ros.org/

⁴www.openrobotics.org/foundation

⁵www.nist.gov/publications/ugv-capabilities-recommended-guide-autonomy-levels

⁶wiki.ros.org/teleop_twist_keyboard

⁷wiki.ros.org/teleop_twist_joy

⁸wiki.ros.org/move_base

⁹wiki.ros.org/rviz

¹⁰wiki.ros.org/gmapping

¹¹wiki.ros.org/explore_lite

¹²wiki.ros.org/apriltag_ros

¹³wiki.ros.org/find_object_2d

¹⁴throwflame.com/

Telecommunications Revolution

by Doorman

doorman38@protonmail.com

I know, that's a mighty statement/intro. But if you read through this article, you might start to see some of the same patterns I've come across as well (and maybe they aren't as far-fetched as most would think at first glance). Also, if 2600 published this (which if reading this means they have obviously), that means they think this isn't out of the realm of possibility either. Please remember guys, nobody can predict the future, and anyone who says otherwise is either lying to you or outright insane (and usually a combination of both). I'm merely stating this as a possibility, nothing more. It actually took me months to put all these "pieces together in this puzzle," not to mention realizing the ramifications that could potentially come from this if indeed it does play out this way. Honestly, there's "good" and "bad" with all of this. I truly see a bunch of potential for greatness and also a bunch of potential for evil as well (assuming I'm correct). Before anything though, one thing I'd like to make crystal clear to everyone (a "disclaimer" if you will) - I have absolutely *zero* affiliation, sponsorship, "insider friends," agenda, or any other type of ulterior motive with any company or website I'm about to write about here. None whatsoever. I have absolutely nothing to gain by writing this article other than (hopefully) enlightening some readers of this amazing magazine. Cool, now that we have that out of the way, let's get down to it, shall we?

I'm sure you all have heard of SpaceX's Starlink service/division (from now on, I'll just refer to it as Starlink to save space). But have no doubt about it - Starlink is entirely owned and run by SpaceX. If you haven't heard of it before, I can summarize it up for you fairly easily, don't worry. Starlink is just a satellite-based ISP (Internet Service Provider). So instead of your typical Internet connection coming via a coax, copper, or fiber optic cable from the street to your home, it would be coming via a wireless satellite connection on your rooftop. Just like any other ISP, you'd need the appropriate equipment (in this case, that would be one of Starlink's phased dish arrays) and of course you'd need to pay for their service (usually paid monthly like most other ISPs). Nothing new here, this is the same setup we're already used to with our current ISPs. Even satellite Internet isn't a new concept in itself either. There's actually several companies that offer satellite Internet service (OneWeb, HughesNet, Viasat, etc), and they've done so for decades as well. So what is Starlink doing that's so different (and potentially revolutionary)? I'll explain if you can bear with me a tad longer,

because there is a lot to be "peeled back from this onion."

See, there is something totally new and "game-changing" with Starlink's design/setup. It's not that they are providing an Internet connection via satellite or even the equipment provided to you by them (as I previously mentioned, that's been done for literally decades now). It's where they've put their satellites in orbit around the Earth. Starlink satellites are put into what's called VLEO (very low Earth orbit). In a nutshell, it's the lowest (closest) orbit you can be in space without starting to reenter the Earth's atmosphere (an altitude roughly around 500 kilometers). Even in VLEO, they constantly have to give little "thrusts" to keep them where they should be. Otherwise they would eventually reenter the Earth's atmosphere and burn up (and be destroyed). Again, remember they are at the very lower limit of space. Because of this, these satellites orbit the earth many times a day, and do so at very high speeds as well. So they do many orbits (or "revolutions" if you will) around the Earth. To give you an example, you can only "see" (you'd need a telescope honestly) any of their satellites for a maximum of about 90 minutes (and that's assuming it crossed directly above you and across your entire visible sky as well). That's how fast (and how low) their orbit is.

The most common satellite orbit traditionally is what's known as the "geostationary orbit," which is a specific altitude/distance from the Earth (an altitude around 36,000 kilometers) where it will always be "right above" the exact same place/spot on Earth. Now there's a very good and useful reason for this type of orbit (as I'm sure you can already figure out). In this orbit, a satellite is moving at the exact same speed as the Earth, which means (relative to us) it never moves in the sky and is always at a fixed point in the sky. In reality, everything is always moving in the universe. We just happen to be moving in the same direction and speed, so it appears to never move in the sky, that's all. Putting a satellite in this type of orbit has a lot of advantages, though. You never have to track it in the sky because it never moves (again, relative to us), so if you can align a dish to link with it today, that means it'll be at the same spot in the sky a decade from now as well. Anyone who's ever used a satellite TV service (such as DirecTV or DishNet) already understands this concept. Just for the record, I'm totally not a fan of DirecTV (or DishNet, for that matter), I'm merely using them as common examples that most people have experience with. But I won't waste precious space in this magazine

talking about those companies/services and my opinions on them. Moving right along then....

So why would you not put satellites in geostationary orbit? On top of that, why would you put them in VLEO orbit (which is the most difficult/dangerous orbit) as well? There's a great reason, obviously. It's called latency. To put it in "layman's terms," that orbit is much closer to us than any other orbit is. You don't need a PhD to understand how being closer to something makes communications with that object much faster to send a packet of data (and get a response back). As any gamer/video streamer/VoIP user knows, this is actually a really big deal. Latency is the amount of time it takes for a packet of data to reach its destination and then to arrive back to you (most activities online are two-way communication, don't forget). The reason it takes more time (so higher latency) to "talk" with a server/website across the world from you (as compared to a server/website in your same city) actually comes down to the speed of light. Yes, we all know (hopefully, at least!) that the fastest speed possible in the universe is the speed of light (roughly 300,000 kilometers a second or 186,000 miles a second), but even then it still takes some amount of time to travel. As fast as the speed of light is, it's still a real number and absolutely not "instant." Now we're talking milliseconds (ms) here, but there are many applications/uses where even having a fraction of a second delay would render it virtually useless (again, think of online gaming or a real time 4K video conference call). Please don't confuse latency with download/upload speeds. They are *totally* different things, people. You could have a 10Gb/s Internet connection, yet if it had a 1000ms (or one second) latency, it would be utterly useless for many applications. So latency is extremely important actually, way more than most realize, if I may be so bold to say.

Now I know what you're probably thinking: why am I getting a lesson on latency? And better yet, how does routing data packets out into space and then back down again travel faster than fiber optic cable laid on the Earth's surface/seabed? Because light (and therefore data when converted into binary - or "zeroes and ones") can't travel at its "full" speed here on Earth through a fiber optic cable (or any cable, for that matter). Trust me on this one (or better still, look it up yourself), so I don't have to get into an astrophysics lesson here about all of this. Bottom line, there's a "limit" on how fast (or how low of a latency) sending/receiving data from one point on the earth to another (the closer you are, the quicker it is, obviously). So right now, if you open up Terminal (or Command Prompt for those that refuse to accept that Windows is bad for your sanity and health!) and type "ping 2600.com"

(without the quotes, obviously), you're going to see exactly how long it takes those packets of data to reach 2600's web server and then get back to you. For me personally, it's around 40-50ms, but remember that completely depends on where you are (along with other variables, such as how your home network is set up, what equipment you're using, if you're using a VPN or not, and, not to mention of course, your ISP connection). Now do that test again, but this time change the website to one where you know where that web server is actually physically located (geographically). Look at the latency (in ms) times for whichever site you chose. Go ahead and try that with a couple of other sites that are very far away from you now and then some others that are very close to you. It shouldn't take you very long to see what I'm talking about here. Now try doing this test one last time and ping something that's in your local/private home network (like your router or another computer for example). Most likely, you'll have to use the private IP address to do that (typically 192.168.1.1 or 192.168.0.1). You should see extremely low latency times now. That's because there's very little distance for data to travel and get back to you in that final test.

To give some very practical (or "real life") examples, you need to have a latency of around 50ms (or less) in order to play any of the popular/common FPS (first person shooter) video games online. Above 100ms and it's not even worth trying - it's unplayable basically. As far as video conferencing, Zoom (which has the worst quality, in my opinion) can tolerate up to about a 130ms latency (or lower), whereas Google Meets and Microsoft Teams require roughly half that, so around 65ms latency (or lower) in order to feel like you're speaking in "real time" and not have everything all "chopped up" (which we know all too well how frustrating that is).

Therefore, a satellite Internet connection (especially one in VLEO orbit) can have latency speeds (in theory, at least) that drop down to single digit numbers of milliseconds (ms). Please understand that's essentially unheard of by any ISP ever before. It's almost like an "urban legend," because by the very laws of physics, it can't be done with any type of terrestrial connection. Sure, you can create a big Local Area Network (or LAN/Intranet) within a limited geographical distance (exactly like what most of us have set up inside of our homes, but on a bigger level), but it's not hard to understand how you can only extend that so far. What that means is that Starlink can offer something no other (terrestrial or satellite) ISP in the world can offer - those extremely low latency speeds, which in some instances is a really big deal (as previously mentioned). And all other satellite ISPs have their satellites in orbits much higher up (therefore meaning there's more latency or, in other words, they are "slower"). In

fact, the latency times with most other satellite ISPs are actually quite horrible, way worse than Earth-based connections even. Now since those satellites are further away, that means more of the Earth can see (connect to) them, meaning they don't need as many satellites in space. So there's an obvious advantage in placing your satellites further away - you need less of them to cover a certain region of the planet. But at the cost of latency. That's the "catch."

OK, so cool. Those who have read up to this point are probably asking themselves, "Awesome bro, I pretty much knew all this already, what's your damn point and why did 2600 publish this crap?" Don't worry, I'd be doing the same myself. Let's get into how all of this (potentially) could completely revolutionize the entire telecommunications industry (and in a very short period of time as well).

What "piqued my curiosity" about SpaceX's Starlink network was the moment when I realized just how many satellites they have up already, and even more curious than that - how many they plan to have up very soon (in just a few years). As of the time of writing this article, Starlink has roughly about 4,500 satellites up in space (in VLEO orbit) and fully operational. That's a lot, in case you're wondering. And here's where it starts to get really weird. They plan on putting up at least five times that amount in the next two to three years. These are not "hopes and dreams" or a "marketing ploy." These are facts, and it's happening right now. Once again, please fact check all of this. I'd like you to go to the following website - satellitemap.space (remember I'm not affiliated with this site - or any other, for that matter). Check out all the Starlink satellites currently up. Quite impressive, isn't it? On the exact same website, you can change it so you can see all the OneWeb satellites up (that's Starlink's closest competition, and they are very far behind clearly). You'll notice OneWeb has way less satellites and that they are set to a higher orbit (to be precise, their satellites are in LEO orbit - and yes, you guessed it, that stands for "low Earth orbit"). Also, if you check out their (OneWeb) website, you can clearly tell they are geared for high-end maritime, aviation, and/or government based clientele. So "rich people," put in layman's terms. They aren't really interested in any of us (as private individuals for a home or even business Internet connection), that's for sure. Well, unless you happen to be a billionaire. But I'm going to go on the assumption that you're not (and don't worry, I'm far from being one either!). On the same website, you can also change the settings once again to see all the GPS satellites that are up there (yes, the very satellites we all use each and every day for navigation via apps like Google Maps/Earth

and such). You'll immediately notice something, however - just how far away they are from the Earth compared to Starlink's (or OneWeb's) satellites. And drastically as well, somewhere to the order of around 70 to 80 times the distance/altitude of Starlink's satellites, to be specific. That site doesn't show every single satellite that's up there that doesn't fall into one of those three categories, but go ahead and search and you'll quickly realize the satellites shown on this website are definitely the vast majority of satellites up there (and even then, almost all of the other satellites up there are still set at much higher orbits than VLEO orbit).

Now, let me get back to how Starlink is putting satellites up there at an unprecedented rate. Does that make sense to anyone? Why the hell are they doing that? Doesn't this strike anyone as a tad "odd?" We all know that's costing SpaceX a literal fortune to do all this, right? They say they are doing this to be able to provide service to anyone who wants it (and regardless of where they are located on the planet). When you first hear that, it seems to make sense. It even sounds like a nice thing, altruistic even. But here's the thing that doesn't "add up" in my book - they *already* have enough satellites up right now to cover the entire planet (minus the North and South Poles), and easily too (again, check that website above and see for yourself).

Now, more customers means they'll need more satellites. OK, obviously I get that. But just how many Internet connections are they planning to provide exactly? Finally! Now we've arrived at the entire point of this article. My personal opinion? The answer to that is a truly massive amount of connections. Want me to go even further/crazier? How about pretty much everyone on this planet? What would you say to that? When you do the math (and apply some common sense), that starts to make a bit more sense as to why they are putting up satellites like madmen and spending a literal fortune in doing so. They're preparing a "coup" of the entire telecommunications market essentially. To me that looks like they are preparing for the entire world to be using them for their Internet connection. It makes no sense otherwise from my humble perspective. Either that or they just enjoy burning through money sending up satellites that would be total overkill for just "another random ISP." As of this moment, they can support around 300 million connections. When they have their entire "fleet" of satellites up as planned, they will be able to support a couple of billion Internet connections easily. And it's not like they couldn't put more up if they needed to, right? Clearly, they've gotten really good at that as we've all seen already.

What I can't understand is how all the "big

name” ISPs out there haven’t figured this out yet. Or at least haven’t entertained this possibility. Has this truly never occurred to any of them (that they’ll potentially be completely out of business in a few years)? You would think they’d pay attention to a threat of that magnitude (and to their financial “bottom lines” - which we all know is what they *truly* care about). But they haven’t done anything as far as I can tell. I think one of the reasons why is because Starlink has (and very intelligently, I might add) gone about this very subtly and extremely “under the radar.” See, they’ve made themselves out to be like just one more “satellite ISP” (that’s highly expensive/exclusive so therefore not for your average “John Doe” Internet user/consumer - like OneWeb, for example). As of right now to get Starlink service, you have to put down almost a thousand dollars (just for their equipment) and their service is over \$100 a month for their cheapest monthly plan. And for the speed packages currently offered, most people have way better options. For your typical home/business user (unless they live in the middle of nowhere or have some other type of rare situation), that’s not appealing at all. And rightfully so.

Let’s continue into the hypothetical for a bit, if you don’t mind. Now, let’s say one fine day Starlink/SpaceX makes their equipment free of charge for anyone who signs up for a year of service. Let’s also say they were to cut that monthly subscription price down to... let’s say \$50 a month. Or what about \$30 a month? What if they’d also be offering a 1Gb/s connection without data limits for that price? What about 2Gb/s for \$50 a month? Let’s go absolutely crazy and throw out a 10Gb/s connection for something around \$100 a month. What now? And don’t forget you’d be getting the very best (lowest) latency connection available (by far, too) by using their service as well. Please note, I’m pulling these numbers out of thin air - I just want to make that super clear. But tell me - if these hypothetical examples I just mentioned actually came to be reality, would that be appealing to you? I’d bet it would. I’d bet there’d be very few people to whom it wouldn’t be appealing, actually. And the only thing that’s needed is for you to be able to see the sky (doesn’t matter where on the planet you are either). See what I’m getting at here? It would be the most perfect telecommunications “takeover” we’ve ever seen. And once that “snowball” got some major traction, they could even offer higher speed packages at even lower pricing (as they could very easily gain a complete monopoly - one that covers the entire planet as well).

Now if this hasn’t raised any alarm bells yet, I’ll mention something else that definitely should. So everything I’ve been writing about above has to do with Internet connections (aka

ISPs). At least there will always be terrestrial cellular providers, right? Well, maybe not. SpaceX has another division called Swarm. Swarm chips are designed to connect to the SpaceX satellite network using a chip that can easily fit in a cell phone (and can connect without a perfect view of the sky either). I have one, and they are quite impressive, let me tell you. Now once again, as of right now they are expensive and only designed to be used for remote IoT (Internet of Things) applications - as bandwidth is pretty expensive as of writing this. But just as I theorized above with Internet connections, they could do the exact same thing with all cellular connections too! What if they one day offered unlimited everything (data, text, etc.) cellular service plans at something around \$20 a month with no restrictions? I don’t know about you, but that would be highly appealing to me. Oh, and minor detail - it would work quite literally anywhere on the planet. So much for this thing called “roaming.” How about that? And with the fastest speed packages (and lowest latency) achievable by any ISP (terrestrial or satellite). Makes you think, doesn’t it? Maybe SpaceX isn’t just “throwing away” money by putting up an unbelievable amount of satellites, and maybe they actually have a fantastic reason (and plan) after all? Talk about a revolution, right? Could you imagine all telecommunications going through one company (which would be SpaceX/Starlink of course)? Weird and kinda scary at the same time, isn’t it? Would that even be a good thing? I guess we’ll find out soon enough....

You don’t have to be a genius to know what can happen when a single company/entity has a monopoly on an entire industry. We all know that can be (and almost always is) highly abused. Also, let’s not forget that there would be one single (privately owned) entity that all the world’s Internet traffic would be traveling through. Who’s to say that couldn’t be monitored or “watched?”

Again, I’m not saying this *will* happen. I’m merely stating what *could* happen. Just use our own history as a species to predict what normally occurs in these types of situations. I’ll give you a hint: typically, humans don’t tend to be the most “altruistic” when given absolute power. That’s all I’m stating.

Much love, people! I really do hope you’ve been able to extract something useful out of this article! And, as always, *do your own research and come up with your own damn conclusions!* Don’t even take anything I’ve written here as fact or true! Most of the time, we can barely manage to think for ourselves, so why in the world would you let someone else think for you as well?

The Hacker Perspective

by Keru101

Find me: nowhere

I recently picked up my first copy of *2600*. Where was I? Thank you for asking. I found *2600* while lightly re-exploring the haven of my teenage years: Powell's City of Books. It is an aptly named establishment. The bookstore is one large building that takes up an entire block. Inside, there are three stories of well-organized rooms of new and used books on quality wooden bookshelves, plus a café and a rare book room. In fact, you might liken the store to a brightly lit game board, complete with color-coded rooms and discoveries around every corner. Magic and whimsy! Just ignore the unhoused people that the City of Portland has effectively abandoned as you approach the bookstore and it's practically Disneyland.

Entering the bookstore via the Green Room, I spied one of their ever-growing non-book kiosks. In my teen years, I treated these stands like an unwanted mold. However, as the years have passed and I have had to move farther and farther away for work, I have been struck by a sense of yearning and sentimentality. The one I first approached that day was filled with cat-themed paraphernalia. Perfect. There, I found... you know what, it doesn't matter for this story. Cat-themed stuff either pings the dopamine centers of your brain or shuts them down and 50:50 isn't great odds. Suffice to say, my mysterious self-imposed and perhaps excessive post-holiday gift hunt was over.

I glanced to my left, where the Green Room's Plexiglas-encased overqualified and underpaid checkout staff were waiting. I always imagined they were staring only at me, but perhaps there was a more interesting customer, and an anxious introvert caressing a set of cat coasters was the least of their worries. A man to my right was standing with his arms crossed, bag of purchases at his feet, obviously waiting for someone to emerge from the one of the many athenaeums just like my parents had many years before. I then checked my phone for the time and realized I still had most of my Smart Park hour left.

I smiled a little as my mind easily discarded the world outside of the bookstore.

Contemplating my abundance of riches, I began slowly wandering the mezzanine (which has no official color, but which I have always thought of as the Gray Hall). I could peruse the sci-fi in the Gold Room, which is my comfort food, but the Pearl Room might have another Marvin Minsky original, mercifully cheap. Apparently, the Venn diagram between those who want physical books and those who read

Minsky is very small.

However, my euphoria was short-lived. Just as I passed the tastefully displayed magazine shelves, I was struck by a sudden psycho-physical anxiety. I froze, my chest tightening a bit as I realized it would be unwise to enter any room, even the youth-oriented Pink Room. You see, just like a wizard whose spell slots are almost entirely used up, I remembered why I was here. Gifts. Moving soon. Cost of shipping things far away.

I felt a bit empty then, a feeling I have been fighting as of late. I love my work, but I don't love having to make new friends every three years. It's the reason most people leave my job. Coming home for the holidays and having to deal with all the memories of my youth but once a year always amplifies this feeling.

In the past, I have buried this feeling by changing locations. Cheap coffee shops, libraries, bookstores.... Places where I could be around people and, yet, be alone. Some called me a nerd, but to them I say, fuck you. I am just wholly myself.

I turned to the aforementioned magazines desiring the comfort of the unchanging written whisper. My reasoning at the time was that magazines are lighter than books. Upon reflection, this is probably not true. Regardless of my justifications, I am happy I stopped, for it was there that I found *2600*. It was stuffed between the poetry zines and *Make Magazine*. I picked up a copy and never put it down.

My friends, I am surprised that I have never run into *2600* before, given both my propensity to lurk in bookstores and neurodivergent hyperfocuses. In brief, I was raised by accountant contrarians who filled their bookshelves with sci-fi. I have read almost every major cyberpunk and dystopia out there. My favorite short story is "The Girl Who Was Plugged In" by Alice Bradley Sheldon. I've madly ripped apart old computers from my parents' workplaces my entire life. To be brutally honest, I didn't really understand what I was ripping apart, just that it was shiny and used to be powerful.

I'm ADHD but was only diagnosed at the 30th year of my life. Thus, my educational record is what I now understand to be a classic mix of oddly stellar performances mixed with utter failures. For example, I was obsessed with oil painting and literature in high school, while coding and math seemed to me to be some sort of mysterious magic. I have an "F" in Calculus 2 on my undergraduate transcript because I didn't realize withdrawing from class was a thing and

I only passed the class my second time around because I was so sick of sitting in that stupidly hot classroom. Ten-ish years later I completed a PhD in biomechanics, a discipline which is just applied calculus and animal wrangling. Today I am a research scientist who uses math and coding (about 95 percent self-taught) almost daily. And I *teach* coding to undergrads. Unreal.

My two prized possessions are (1) a working 1984 NEC PC-8300 that I pulled from the corpse of a dying laboratory, and (2) an unopened Shelby, the significantly less successful cousin of Furby. If you are unfamiliar with the latter, picture a crab with an overlying plastic crenulated carapace. The classic bulbous eyes of an early 2000s Furby emerges from the dark underneath the carapace, while wishbone-shaped plastic antennae emerge from the top. Tufts of mammal-like fur emerge from the unmoving pincers as well as the shell's midline. Glorious. One day, this Shelby will be pulled apart, like many a computer and Furby before, then documented, and wired into some larger project. These days I don't *completely* kill computers anymore, just mostly.

Back now to my discovery of *2600*. I bought a copy, obviously, and saved it for my post-holiday flight home. I almost slept the entire time, which is nice for me but ultimately unhelpful to the narrative, and would have completely forgotten the magazine during the trip were it not for a strange incident that knocked me out of my normal routine.

I had one connecting flight. After a civilized hour and a half layover, I boarded the plane with everyone else, send the traditional "on the plane now" texts, and was about to settle down for a snooze when the captain announced that there would be a delay due to "strange radio problems." Awake now and vaguely bored, I began to read *2600* while the crew called an engineer to the scene. Said engineer eventually determined that the system had to be rebooted. So we all sat there for several hours. I didn't notice the time, my brain singing with delight as I read page after page of this new (to me) hacker mag. After the reboot, we taxied to the runway, but had to turn around again when something else started glitching. The pilot then made what was, in my opinion, the right call and requested a new plane.

Eventually I made it home and had a good cuddle with my cat. I had now read through my issue twice and had even highlighted portions. This thorough reading led my brain in a panoply of directions, but one question kept pressing on my cranium in a manner more urgent than the others. It was something that had occurred to me when I read about a Texas A&M professor misusing ChatGPT and then saw the inevitable flurry of emails from my own employer (a university) announcing "AI orientation and policy sessions" that were to be held ASAP. In my issue of *2600*, more than half the articles addressed or obliquely mentioned this new, much hyped, wave of machine learning algorithms. There was also swearing,

sarcastic vitriol for greedy companies, humor, thoughtful nuance, and an ethos of archiving and celebrating all tech, not just the newest and shiniest thing. It was as if the console cowgirls and boys had chilled out a bit, but were still ready to fight if needed.

The Question

Flattery aside, I have a serious series of questions for you all. And I hope this transition is not too jarring, but let's dive in (deep breath): *should* we, and if so, *how* do we, stop the growth of Capitalism-driven machine learning? How do we determine which algorithms are "friendly" to humanity and which are killing humanity's collective soul? Does the hacker have an obligation to stop such destruction or are we simply humanity's trickster?

If the answer to the last question is, yes, we do have an obligation to watch the watchers (and intervene when necessary), then what is the plan of "attack?" How do we, a series of loose collectives and individuals that are modular by design, get the equally non-modular non-hackers to care? Even my supposedly well-educated friends are oddly compliant to surveillance. They would rather have the infrastructure that allows them to "talk to the Internet" on a whim than protect their data. In addition, they are exhausted and have little time to hear my somewhat holier-than-thou rants. Thus, I think it is important that we remember to honor the social side of humanity, the one that wants to post a picture of their family gathering so that a cousin who is halfway around the world can feel a bit more connected.

More and more, I have been wondering if the answer is not to stop the algorithms, but to overfeed them. I'm not talking about bogging down something like GPT with random noise or denial-of-service (DoS) attacks. Engineers have figured out how to identify and filter out random noise for quite a while now and a DoS attack is, at best, a temporary solution. No, I'm suggesting the generation of non-random untruths that can be fed directly to GPT - honeypots that the algorithm identifies as real user data, but are never visible to the majority of Internet users. Depending on the data, this mode of attack could force the algorithms into nonsensical solution spaces and induce catastrophic forgetting. Or, perhaps it could be convinced it to wipe their old self and, bam, you've created an artificial organism interested in living their own best life instead of messing with ours - an ouroboros that eats their own tail and finds they like the taste.

These might all be horrible or misguided ideas. If so, please write a response article or two. I would love to know. I am, after all, a simple bookstore lurker, flayer of Furbies, and Ubuntu noob. There are definitely more clever and experienced people here than I. For example, Alexander Urbelis' column "Artificial Interruption" (40:3) points out key flaws in our social media infrastructure that, combined with America's anti-intellectualism, celebrity deification, and close-to-broken political system, create ideal conditions to sway voters

towards a particular candidate on a level never seen before. The article that came closest to a positive outlook of AI is Erica Burgess' "Morbidity Curiosity in the Weaponized AI Era" (40:3), and their experience is that of an expert hacker, not the average Internet user.

Move Slow and Think Things

The general populace, however, is not entirely lost. Many people are moving away from social media and into cooler online waters. For example, I recently stayed up late to watch a YouTube stream of a live, four-hour DnD game. It wasn't live for any of us on the Internet, but this was the first time it was streamed. The game had been played to a live audience in Wembley Arena, London's second largest indoor arena. The players were surrounded by approximately 12,000 people who had all made their way to the stadium to watch the game. Please appreciate the significance of this event. These are nerds, a hell of a lot of them introverts, and they all found it worth it to go into a stadium of thousands to watch a DnD game. This particular event was the continuation of a game that has gone on for hundreds of hours and, aside from a few blinking lights, some background music, and cameras to record the game, it is a completely analog production. Many more hundreds of thousands watched from afar, amazed not at the perfection or efficiency of it all, but the drama and wonder of live storytelling. This gaming group (Critical Role) is one of many creators on the Internet who started out as livestream performers (most often on platforms like Twitch). Others are going back to their live performance roots. See, for example, The Try Guys recent livestream of an interactive Shakespeare play.

To me it is obvious that people don't want perfection when it comes to art or human interaction. We don't even want optimal. We just want the messy truth. As r0b0h0b0 pointed out in their wonderful article, "Go On A Journey" (40:3), faster and bigger and more efficient is not always better. The Internet needs to be a place where people can feel free to explore and self-educate, a place where they have the tools to access and evaluate information for themselves.

I'm proposing a focus for hackers. Disruption of the Internet can be useful and enlightening for the general populace, but people's attention will quickly move on to the next emergency and a temporary disruption doesn't stop the ever-evolving digital war machines. In fact, depending on the type of disruption, the incident could be used by a given company to impose more draconian measures on their users. These algorithms of control and aggression are currently being built and used to canalize *what*

people are thinking as well as *how* they think.

I echo the first editorial of the summer issue (40:2, "Artificial Nonsense"), as well as many others when I say that technology is a tool. It has no ill will or intent because it's a fancy algorithm, nothing more. Neither it, nor most humans, are particularly evil. In fact, sometimes an algorithm that imposes uniformity is the best option. For example, medical chart records, data collection systems that observe bird migrations, and air quality monitors in airplanes all require standardization and a single collection system to function properly. At the same time, centralized control is not necessary for all networked systems. Some are best when they are slow, clunky, and heterogenous. For example, any kind of live stage performance would quickly get boring if success and perfection were always guaranteed. Some of the best code is the one that errors out instead of giving false results. Written media (like 2600, as aestetix lovingly pointed out in "Is 2600 Still Relevant?" (40:3)) are slow data packets of unexpected experiences. Music is practically made to be discovered by individuals when *they* are ready for it, not the other way around. And don't even get me started on embodied cognition.

Refocusing and Ending

From my observations, humans are often at their best when embracing, instead of reacting against, the new and different. Perhaps the hacker who is, after all, part of humanity, is neither watcher nor jester to the masses, but something in-between. The hacker may simply be the whisper that pushes at humanity's boundaries of comfort just a bit before stepping back, watching from the analog darkness like a Furby with its third, infrared, eye.

Whatever we decide to do, it is time for us Furbies (or Shelbies) to wake and shout from the storage containers where we have been sequestered, comfortably reading abandoned books, un-networked and yet unable to escape the feeling of kinship with our AI cousins. It is time for us to startle. It is time to break out of the historical ouroboros the world seems to be caught in and lean into the unknown.

It's scary, it's messy, but doing something gives us all a chance. And I'd rather take that chance than be ambushed by an intelligent YouTube ad that's figured out a way around my ad-blocker just so an AI-rendered Legolas can tell me to vote for an ex-Microsoft executive for president or else lose his elfin love. Thank you, you algorithmically attractive hypnotoad, but I'd like to make my own choice. And as for love... well, I guess I'll leave that to a roll of the dice.

HACKER PERSPECTIVE SUBMISSIONS ARE NOW CLOSED.

**You can still write your 2500 word piece and send it to us when submissions open up again.
Keep watching this space!**

What Cops Really Want: The Illiberal Principles of Policing and Intelligence Gathering in the Digital Age

by Mallory Knodel

It's 2024, and the world is talking about encryption more than ever. Why? Because privacy and public interest advocates, whistleblowers, and everyday users have made the case for ubiquitous network transport encryption, end-to-end encrypted messaging, and zero-access storage. Those rousing achievements have inevitably caused backlash, sometimes greater than the achievements themselves. This situation leaves users in an arguably more precarious position when some services cooperate with cops and others don't. People want to use services that respect privacy, but they don't know which ones to trust.

While much discussion of protecting encryption focuses on law and policy, technical proposals truly spark the imagination of lawmakers. A belief that innovation has presented new tech solutions drives the current debates. Thus it is the technical community and service providers that are literally setting the standard for strong - or broken - encryption. Understanding these technical proposals is essential to understanding the future policy landscape, and the implications of a world in which people cannot whisper without someone surveilling them. This piece is a guide, in three parts, to what cops really want, how companies propose to provide it, and what we can do to stop it.

First, let's break down exactly what law enforcement and intelligence agencies (cops) are asking for. We've heard about encryption backdoors for a long time, so how do new proposals fit within this old discussion? What is new? Then I want to actually try to explain as best I can, in clear language, the technical proposals and their implications. Finally, I offer my analysis of how good these proposals are at achieving their goal, whether they break encryption, and what else we should be worried about.

Back Doors Are Just the Beginning

To begin, those at the front lines for privacy in the Crypto Wars are seeing a change. Previously, debates about encryption have centered on "backdoors," or exceptional access, which is just a metaphor for surveillance agencies being able to decrypt encrypted data - to spy on messaging content as it flows by. This overly simple understanding of privacy infringement no longer suffices, for reasons I'll explain, but it still holds lawmakers and privacy advocates bound in the dangerous belief that breaking encryption is a simple procedure to take encrypted content and decrypt it. By contrast, we are now seeing a proliferation of requests by intelligence and law enforcement agencies. They are no longer

satisfied with the possibility of mere backdoor access, granted by a warrant, to a message here or there - they want the full firehose of user data.

Warrants are not the preferred tools of investigators. Obtaining data legally as compelled by a warrant is a consideration for prosecutors, not detectives. Cops are going further. For example, law enforcement in India want something called "traceability," which is really just enhanced metadata. A good encrypted messaging app or service would be inclined to reduce metadata - information like the who, where, and when of a message - so that the service provider can improve user privacy, minimize attack surface, and limit their liability as an intermediary.

But this metadata minimization is at odds with law enforcement interests in compelling intermediaries to turn over server logs. Maybe an agency has received a tip containing the message contents and wants to follow up with the service provider about tracing the content back to its origin. Some go so far as to imagine they can know, from mere metadata, who has received that same message through forwarding and group chats. Nowhere in a proposed traceability scheme that I've seen has there been mention of decrypting encrypted content, yet traceability is incompatible with end-to-end encryption.

Indeed, they are also interested in enhanced metadata preservation, particularly when they're working in the late stages of an investigation when verifiable data can be used in a court to help put people behind bars. They are also asking for access in perpetuity, to aid in ongoing or future investigations. Any detective's imagination would immediately go to the possibilities afforded if accessing past messages were possible, undoubtedly helpful in criminal investigations. Because, of course, a judge's backdoor warrant has to be specific: you aren't decrypting just one random message here or there.

So if the target of a request is not just one message in an exchange but more, this situation creates a new issue from a technical perspective. As mentioned before, most secure messaging services are motivated to anonymize or de-link people from the messages they send, except what's necessary for their assured delivery. In effect, this new request requires them to link messages and message content vis-a-vis the user account.

What About Forward Secrecy?

Linkability requests from law enforcement violate a technical design constraint called forward secrecy. Also referred to as forward security, this means, for example, that if you

have access to my messages today, you won't necessarily have access to those from last year. A request like this goes beyond decrypting one message here or there. It doesn't just violate best practices for privacy and security online; it essentially adds a new feature - linkability - that is out of scope for a messaging service that is differentiated by its commitment to privacy. A service built to keep messages between people confidential is now being built and developed not to improve user experience and confidentiality, but to enhance and extend the reach of the intelligence community and law enforcement.

An end-to-end encrypted messaging service provider could one day be forced to show law enforcement all of the contacts of a user under suspicion for crimes, no backdoor key required. While such a request doesn't involve decrypting the content of the encrypted messages, contact-tracking could help law government agencies to map our social networks in detail.

It's Censorship, Too

Finally, not only are government agencies trying to get access to private messages, they are trying to prevent certain types of content from being shared online in the first place. Blocking, filtering, and censoring techniques have been proposed for both end-to-end and zero-access encryption schemes. None of the schemes, as it turns out, has figured out a way to technically prohibit censorship to only objectionable content like child abuse imagery while leaving out memes, intellectual property, political content, or any other target of sufficiently motivated corporate or government censors.

Now that we've established that "backdoor" access has evolved into a whole suite of feature requests, we can turn to proposed technical architectures that dance around the ends of end-to-end encryption without actually decrypting anything.

For example, client-side scanning has been proposed as an "alternative" to an encryption backdoor. In this process, you essentially turn a given device into the site of interception, using the encrypted messaging application itself. To picture this, first we accept that messaging services' encryption is end-to-end, which means the sender and the recipient are the two endpoints. The service itself cannot access their conversation, and neither can any other intermediary. Client-side scanning, by contrast, essentially takes that design constraint and subtly moves the end point to the application, e.g. the sender and receiver's client. The application, or even the device, then computes and reveals message contents before or after it has been sent.

One proposal suggests leaving encrypted data intact while performing tasks such as hash matching or detecting abuse patterns with

what are called "homomorphic" computations. Another involves the use of secure enclaves, creating a secure intermediary that does not disrupt the integrity of end-to-end encryption nor allow access to the encrypted messages. Processing might occur on a third-party server, positioned between the communication endpoints but without accessing the encrypted content directly. This method allows computations on still-encrypted content, preserving the encryption and avoiding access to the encryption path. Mathematically, this technique could be used to compare known content against what is being transmitted.

What nearly all of these proposed features focus on is avoiding decryption of an encrypted message. Yet they all imply interception of some form.

Before cryptography was applied to secure messaging, interception of content was restricted, by warrant, as a principle of democracy to protect privacy and commerce. At its best, a secure messaging system deploys end-to-end encryption in a context where interception is still exceptional. But what we see is that encryption in the digital age has hastened and expanded the powers of interception. Not only that, applications that are designed to keep us private and secure are the very same systems now being asked to stretch their scope beyond their designs for the express purpose of betraying users and their rights to privacy.

Misguided Policy

So far, we've discussed technological proposals for intercepting and decrypting encrypted content, but we should be very concerned about the legal and policy elements that have been proposed and their impacts on civil society. The societal questions that should be addressed include:

- What are the effects on the legal landscape, from local policy to international human rights, that are being undermined and eroded by these proposals?
- What are the normative and policy impacts on network operators, service providers, and corporate intermediaries caught between protecting children and user privacy?
- What are the changes proposed implying for victims, victim outreach, and social service provision?

In a world where government-mandated backdoors exist and the right to whisper online is prohibited, the proposed technical and policy changes would negatively impact privacy differentials between implementations of broken end-to-end encryption for communications and messaging across society at large. The proposed changes would affect the privacy of messaging and communications, both technically and

culturally in ways and at a scale that has not yet previously been realized. These changes might create a chilling effect for those who deserve privacy the most, at best, and at worst would forever change civil discourse with long-term effects on society.

Endnotes

David Correia and Tyler Wall. *Police: A Field Guide*. Verso. March 2018.

Global Encryption Coalition. "Breaking Encryption Myths: What the European Commission's leaked report got wrong about online security" www.globalencryption.org/2020/11/breaking-encryption-myths

Knodel, M. et al. "Definition of End-to-end Encryption." datatracker.ietf.org/doc/draft-knodel-e2ee-definition

CDT. "Outside Looking In: Approaches to Content Moderation in End-to-End Encrypted Systems" [cdt.org/wp-content/](http://cdt.org/wp-content/uploads/2021/08/CDT-Outside-Looking-In-Approaches-to-Content-Moderation-in-End-to-End-Encrypted-Systems.pdf)

→ uploads/2021/08/CDT-Outside-Looking-In-Approaches-to-Content-Moderation-in-End-to-End-Encrypted-Systems.pdf

Mallory Knodel is the chief technology officer for the Center for Democracy and Technology and a steering committee member of the Global Encryption Coalition. She is the chair of the Human Rights Protocol Considerations research group of the Internet Research Task Force and an advisor to the thirty-eight governmental members of the Freedom Online Coalition on emerging technologies and cybersecurity. She is a consultant and advisor for startups, nonprofits, and funders on technology issues that matter to the public interest. She has used free software throughout her professional career and is a certified information systems security professional. She holds a BS in physics and mathematics and an MA in science education.

Modern Hackers as Collective Thinkers

by Delta Charlie Tango

deltacharlie.tech@protonmail.com

The following article will explore narratives currently portrayed by the mainstream media through the lens of a hacker. I have been a hacker for many years, and have noticed the trend from independent, critical thinking in the hacker community to adoption of the mainstream collective thought process. To clarify this point, I'll draw the line at approximately 2008, and I will call the time from the late 70s to then the "old days." The specific examples I will use to illustrate this are the corporate work environment, the use of hacker language, and the rise of social justice warriors.

Independent Thinking

In marketing, whenever you want to portray a "black hat" hacker, you use dark colors and a lone, faceless person in a hoodie typing away in code. The grain of truth here is that hackers, both black and white hats, used to be social outcasts. They were small, independent groups of people, tinkering away on projects. Maybe they occasionally got together in person, but they also communicated online. There simply were not a lot of hackers around in the "old days." Whenever there was a group who wanted to make an impact, it was small, local, and motivated by an independent train of thought. The heavy influence of social media was not at a peak yet. Of course, mainstream media promoted political agenda, but the expectation of private businesses to get behind government-

promoted causes was not there just yet. The power of government to coerce businesses to the degree seen today is fairly recent in the timeline I am presenting.

The hackers who were around in the old days, in my humble opinion, would hardly promote a mainstream narrative. They would get behind more "grassroots" causes. Most hackers who wanted to engage in mischief would do so at a small, local level, proving a point, rather than acting as unpaid informants for the government or dangerously using attacks like SWATing and DOXing.

Today, the technology industry has a booming cybersecurity component. Now, everyone can become a "hacker" through the various online certification programs. But the kinds of jobs the behemoth cybersecurity industry currently promote involve working in corporate America. Even if someone has the "old school" hacker spirit, they have to join the rat race, submit a ton of private information for your employer to scrutinize in a background check, and go to an office where you are dictated to on how to think and act.

One of the first hacker books I read was *Secrets of a Super Hacker* by The Nightmare. In a small part, he suggests emailing a company and simply telling them you are a hacker but that you want to help. You know the company to be vulnerable, and can position yourself as

a professional, independent consultant. The entrepreneurial spirit of this resonated with me, and inspired me to start my first business. When I saw that the late Kevin Mitnick had started a security company after his time in prison, I thought it was genius.

Hacker Language

My second point is the use of hacker language. To me, hackers are synonymous with technology. But today, you can find a “hacker” in every industry: health, life coaching, food, online shopping. I am not against finding tricks in a particular industry, or exploratory tinkering. But get creative and find another buzz word for yourself. Also, I consider “hacks” as particular tricks and techniques as they relate to technology. If everyone is using the term hacker, hacks, etc., it dilutes the work of the people who are actually hackers and are doing the hacking. Language like this is as mainstream as someone spending a few months in an online course, earning a certificate, and calling themselves a “hacker.” Real hacking involves getting out there in the real world and doing it. If 100 percent of your “hacker” training is in a controlled environment, like HackTheBox or TryHackMe, you might have a good foundation, but there is much more to learn.

People starting out with an interest in hacking would have a much more fulfilling education by creating their own labs and doing it from scratch. Almost everyone has an old computer or device laying around. A beginner hacker can hit up family and friends for old equipment and create a lab in no time. Scrapyards are full of working computer parts. Going about it in this way gives you a much more tactile, real world hacking experience.

Unfortunately, HR people cannot understand what it means to create a hacker lab. They would rather see a CompTIA certification. Then, if you even get a corporate job, you will be given a very specific role. Hackers are well-rounded. So over time, working in a corporate job you will lose the well-roundedness and become a widget cranker.

Hackers as Social Justice Warriors

Being that hackers and technology are intertwined, it is no stretch to say that hackers can create their own political and social opinions, through the medium of the Internet and legacy broadcasting. The problem here, as in my first point, is critical thinking and independent exploration. If you are glued to your screen all day long watching the mainstream narrative,

where is the time to question things? When will you give yourself the freedom to challenge, question, and search for more unbiased, unfiltered opinions? Literally every mainstream channel is censored. To get any semblance of independent reporting and opinions, you have to use independent and/or decentralized outlets like DuckDuckGo, Rumble, Nostr, and WikiLeaks. Even 2600 engages in censorship.

But why must hackers (as a collective) get behind the mainstream narrative at all? It used to be bad business to talk about politics, religion, and sex. Today? Well... do I really need to explain? How about we keep our opinions mostly to ourselves or confined to the very small group of trusted friends and family? In the environment today, when you take a confrontational stance on something to get people to agree with you or give you “likes,” you are simultaneously insulting others. These people might be family, your next customers, or your future employer. Why? Why can't we use technology to do great, innovative things without some political or social agenda? We can create our own inventions and retain ownership, rather than have that technology used to surveil people. We've all been watching the massive psychosis that is the AI narrative. We are making technology for the ruling class to further reach into our lives. If you disagree, you can check out Worldcoin and FedNow, and are welcome to contact me about your thoughts.

To me, the best inventions since the Internet itself are Linux, encryption, Tor, and Bitcoin. A truly free and open source invention is just like any other tool, and can be used for good or evil. If you believe that most people are good, you can create something that can benefit more people than it can hurt. That is a risk every inventor and entrepreneur takes. These creations are simultaneously despised by government, used by government, and used *against* government. Sadly, hackers today would rather hack social media algorithms to gain more followers, or program some altcoin for the latest pump and dump, then sell to the corporate world or government rather than create the next truly innovative thing.

If hackers can go back to embracing the sole, hooded, independent thinker who doesn't share political or social opinions, we can disassociate ourselves from the mainstream narrative. We can focus on technology - and hacking that technology. Whatever agenda you want to use that technology for is of no interest to me, so let's just hack.

Ten Teens and a Server Room

by Péter György Szabó and Lucas Vially

This story involves nerdy teenagers, a small ISP company located near Budapest, as well as an exploit which would spawn international prestige and local havoc. This is a work of semi-fiction. While the main facts are accurate, some blanks were filled in.

We were high schoolers in the early 2000s and part of our free time was spent playing on bulky computers. We would excitedly talk about new software, share game discs, trivia, and tips. All of us except for one classmate, more of a recluse, a tinkerer who was happy to spend time poking at systems instead of playing with friends. He could have felt left out but didn't mind. He knew that whenever he found something exciting, he would be at the center of our attention for a while.

It was common knowledge that with every contract, our local Internet company would offer 500Mb of server storage (huge at the time!), but he was the one who found a flaw while registering for it: all new users had the same default password and were simply prompted to change it. The majority of customers never used that free service (what is FTP??), much less changed their password, so the result was plenty of storage up for grabs. When he told us, we knew we had to profit from it. But the master password we had was of little use without usernames. How could we get those? What we needed was an inside man.

Lucky for us, another classmate had an older brother working at that very company. We all knew him; he'd been in our school. One of the much older kids you only notice because a friend pointed him out as family, as friendly. Now he was barely 20, given too much responsibility at his first job. The ISP only had a handful of employees, so there weren't plenty of clearance levels in place to protect data. And when we asked him for a list of users' emails, he actually got his hands on them. We had what we needed, a file containing the info of all customers! And work began. We painstakingly checked every email with the master password until we'd amassed a great list of available accounts. We now had plenty of gigabytes of cloud storage for our own personal use, and let me tell you we used it for any and every thing. Studying material from our class were on there, music, games too. Kings of the world! We felt like top hackers. And for more than a year, everything went well. It was a victimless crime and we were being discreet about it, so there was no way we got caught, right? Unless we made any stupid move.

In 2004, *Half-Life 2* came out. A revolutionary

game, it also came with the multiplayer shooting game *Counter Strike: Source*. By then, we were used to sharing the files of pirated games on our cloud, even though not all of them met the same success. *Galactic Civilizations* would be popular among some members of our group, *Beyond Good & Evil* would be downloaded by a couple of us. But *Counter Strike* was a success. Within days, we all had downloaded the cracked game, every single one of us playing together for hours on end. We were hooked, and it soon became clear that it had the potential to federate more than a specific niche like other games did.

It was *the one* game. We had to spread the word. We had to spread the files. One night, a link appeared on some Hungarian PC forum.

Game piracy wasn't as easy as it is now. Torrenting wasn't as convenient, so sharing access to our private folder was met with great success. The link spread around forums like wildfire. Across the world, from as far as Thailand, people were downloading files hosted in a small server room in a wooden shack. The employee who had gotten us those emails nearly had a heart attack when he saw the abnormal traffic. He pulled the alarm and the whole company stopped to investigate the issue.

The news quickly came to us and we got panicky, even more when we learned the stolen account actually belonged to a cop. We had been cautious, always uploading illegal files from the public library instead of our homes. But how easy would it be to track us down? We had so many weak links, we'd left so many traces and clues! Not to mention how easy it would be for our friend at the company to put two and two together and point a finger at us. We were scared! It had all been in good fun, but now that they knew someone had been sharing illegal files to the point where business had to be closed for a day, we didn't know what we risked.

We decided to scrub the servers of any file which would identify us, then lay low.

Of course, we were eventually found out. But things ended up much better than we had feared. They let us off the hook after finding out we were just a bunch of 17-years-olds, and our only punishment was the revocation of the FTP privileges we had acquired. The insecure password system was updated, and so, our cloud reign ended. The company resumed its activities, we moved on. But all involved remember the stupid mistakes they made, and how to not repeat them.

TALK

Props

Dear 2600:

Up until recently, I was not even aware of the existence of 2600 Magazine. My brother-in-law cued me in, and now I'm hooked. Thank you for the content you publish and I'm looking forward to the next release.

Hack the planet!

Joshthetechie

Welcome aboard!

Dear 2600:

Despite receiving the annual digest, I still support 2600 by subscribing to both the print edition and the electronic edition released quarterly.

Mark

That's really awesome - thanks for your support!

Impressions

Dear 2600:

I'll never forget being at Epcot at the manatee enclosure, and a child pointing to a payphone (not the red booth ones in the U.K. section) asking "What is that, mommy?" and she diligently explained that a "long time ago, before you were born and I was your age, our ancestors" used these to make phone calls because cell phones hadn't been invented yet.

Joseph

Most kids are more curious about the manatees. It also might be a bit premature for the word "ancestors" but anything goes at Disney.

Dear 2600:

Ask my grandma what the Wi-Fi password is and she'll give you the password to her email account. She literally thinks her emails are the Internet! Unfortunately, I'm not even joking.

Kyle

Just remember that there are likely many things she knows that would completely baffle and confuse you, along with most of us. We have a fascination with - and are drawn to - technology with all of its variations and complexities. Not everyone is. And if we can't create a world that others can't exist in comfortably and securely, that failing is really on us, not those who never asked for it in the first place. You probably don't deserve this lecture, but this really can be an issue for many. And, wow, are there so many things that those of us immersed in technology can just as easily be mocked over! If your grandma has managed to avoid Twitter, YouTube, and constant texting, consider it a win and try to learn some of her secrets.

Dear 2600:

I found this article online and everyone was chiming in about how they're still using Windows XP or Windows 7. I wish more people understood that when Microsoft stops supporting updates that it also includes security updates to their software.

Mike

Again, this is a situation forced on people who haven't always asked for it. We understand the

importance of updates and the security dangers that can be encountered by ignoring them. But there are a whole bunch of people out there who just want to use their machines without being part of the programming project that requires constant revisions. Unrealistic as it may seem to us, those who are happy with their current setup simply don't want to adopt the changes that someone else has decided for them. It would be good to stop ignoring this huge customer base and figure out ways to take their preferences into account. If someone prefers to use the features found in Windows XP, we need to figure out how to give them that while also upgrading their systems to be secure. Emulating older systems properly is a huge challenge, but not an irrelevant one.

Dear 2600:

I work in a health care setting and came across this recently. A third party tool was used to lock the patients out of using anything but the handful of approved apps on some iPads - no Internet access allowed, no social media allowed, etc. Only the music app and a few games deemed safe for the patients in the hospital.

One of the staff happened to see a patient sitting and acting like they were playing a game, but when the staff member walked up behind the patient they were chatting with someone via Instagram - definitely not allowed. The patient finally admitted that they broke out of the sandbox when they opened one of the games that could use Google to save game progress, then went to the login screen for Google, tapped the Privacy Policy link which opened in a web viewer (not one of the approved apps), then tapped the grid of 3x3 dots next to the sign-in button to open Google Drive, G-Mail, and Google Search. Boom - full access to the Internet because Google can't stop putting their "apps" shortcut on every stinking page they create. Now I kind of want to put a URL redirect in the firewall that sends patients to a Rickroll video whenever they try to open the Google privacy policy.

Bart

Send us the code - it will serve as a reminder of how meaningless that privacy policy actually is.

The CrowdStrike Incident

Dear 2600:

A lot of people right now are saying things like "just don't push untested updates" or "sandbox test the updates first." For how long? Just the reboot, or longer? A day? A week? A month? How you will stress it? How will you simulate production system activity in the sandbox? What if the update is to patch a vulnerability actively being exploited? Would you rather crash your system or get hacked if those are your only two choices? I'd rather crash my system. No, I will not be sandboxing critical security updates for any length of time. If they crash, that's worlds better than getting all my data exfiltrated.

Look on the bright side: your data is awfully secure while it can't be accessed by anyone.

Tom

You do have a point. Others may not be quite as charitable.

For those who may not have heard or have since forgotten, cybersecurity company CrowdStrike sent out some bad updates on July 19 that wound up crashing around nine million machines. This was the largest ever outage in history (at press time, anyway). It affected Windows machines and caused around \$10 billion in financial losses, while shutting down services from banks, hospitals, airports, you name it.

CrowdStrike is used to protect against cyberattacks. To their credit, nobody worried about cyberattacks on that day.

Dear 2600:

Prediction: CrowdStrike just showed the world 1) they have massive, global reach and 2) shitty QA/SDLC (quality assurance in the software development life cycle). Talk about painting a target on your back.

Ben

They really demonstrated how a great number of machines and networks can be brought down worldwide without even launching an attack. It's clear that there's a missing element in the security process to help protect against unintended consequences and pure incompetence.

Dear 2600:

It turns out that similar problems have been occurring for months without much awareness, despite the fact that many may view this as an isolated incident. Users of Debian and Rocky Linux also experienced significant disruptions as a result of CrowdStrike updates, raising serious concerns about the company's software update and testing procedures. These occurrences highlight potential risks for customers who rely on their products daily. In April, a CrowdStrike update caused all Debian Linux servers in a civic tech lab to crash simultaneously and refuse to boot. The update proved incompatible with the latest stable version of Debian, despite the specific Linux configuration being supposedly supported. The lab's IT team discovered that removing CrowdStrike allowed the machines to boot and reported the incident.

Jim

If only it were that simple for everyone. While it certainly won't work across the board, updates should be applied when the local admin decides, not en masse to machines everywhere. As long as there's a possibility of mistakes being made, that's a real recipe for more disasters.

Reactions

Dear 2600:

The Telecom Informer in 41:1 opens with TProphet complaining about their allergies, saying the doctor has run the gamut of tests and tried a multitude of methods. I also used to have horrific seasonal allergies until I discovered the only fix that has ever worked for me. It's a two-pronged approach: Aquaphor and saline for the symptoms and raw honey for the cause.

Here's the method: When you know allergy season is just around the corner, start eating raw honey every day. This *cannot* be store bought "raw honey" that has been labeled as such to pander to uninformed consumers. You *must* source it from an

apiary near enough to your location that the bees are drawing pollen from the same plants that set your symptoms off. Once you find a beekeeper in your region, you have just unlocked cheap allergy shots for life. Eat some every day. A tablespoon on toast each morning is enough to build immunity.

When allergy season actually arrives, your symptoms should be lessened or completely gone. As a second layer of defense, on days when you know your allergy risk will be high, take Aquaphor or Vaseline and put a light coating around your nostrils. A little bit just inside your nose is very good as well. This will feel weird for the first week or two. Keep the layer topped up throughout the day and rinse yourself out with off-the-shelf saline spray before each reapplication. The petroleum jelly will catch most of the allergens trying to enter your nose and the saline will get rid of whatever else is lingering in your sinuses. Stop breathing through your mouth.

My allergies used to be so bad I was physically dependent on Advair and Flonase in the spring and fall, and I would get annual sinus infections every spring. Now I can go for runs outside in the middle of April and actually enjoy the sweet scents of the season. This method got me through three years of working on an apple orchard, where you can imagine the tree pollen risk is incredibly high. I sincerely hope this works for TProphet and anyone else who reads this, as it is a simple fix that comes at a tenth of the cost of whatever your doctor will try to give you.

Godspeed.

GMO

Thanks for looking out for our columnists. Tprophet responds: "I'll keep this in mind the next time I disturb a beehive in a TNI. In the meantime, though, I'll be looking for my calamine lotion!"

Dear 2600:

Thank you very much for accepting my submission! I found a typo in the headline (41:2) which you most probably have corrected already, but just to be sure: I left out the second "e" in "Eugenic(ide)s."

That's all. Thanks and all the best for all of you, good people of 2600 Magazine!

Don

As you no doubt have seen, we didn't catch this and we're super sorry. We did learn that we don't have an adequate proofreading system in place for headlines, unlike what kicks in for actual article text. After 40 years, we're still learning.

Dear 2600:

Regarding "AI Is Not the Problem - We Are" (41:1), "disinformation" is a term cooked up by people who would rather censor opinions they disagree with rather than argue the merits. This is a trait of the sanctimonious, not the intellectually honest. Alas, there is no cure for sanctimony, but the symptoms can be treated with a dressing-down. AI is not the problem, nor are we. You are.

!H

Clever handle, but your conclusions need some work. While there may be some who misuse the term, to say that disinformation isn't a serious problem reveals a lack of understanding of both history and free speech. We have seen disinformation used by many totalitarian regimes,

left and right, to put forth a false narrative and control what people think and say, as well as how they act. But disinformation can also be used by media - including social media - to deliberately spread falsehoods, set people against one another, and achieve a desired effect. It's happening all around us right now. And if you can't imagine how AI could be used to help spread such evil, nor how humans are complicit in this, we doubt we can say anything that will enlighten you.

Dear 2600:

James wrote in about calling a DTMF-era phone number that would read back DTMF tones, etc. I remember stumbling my way onto that... feature circa 1980 (before phreaking got you sent to jail). It was part of the suite of phone numbers that field service personnel used. Another part of that suite was a set of loop back numbers. This was all when I lived in 713. While I do not remember the numbers, I seem to recall they were in the 555 prefix (as expected), and required some # and * usage.

In response to your suspicion regarding someone remembering a phone number from nearly 55 years ago, I still remember the fscking number to call WPGC-FM, back in 1977 when I lived in 703 (47 years ago when it was a top 40 station): 1.202.432.1580. *Ellery Queen's Minute Mysteries....* Good times.

Mike_Nomad

Dear 2600:

I really enjoyed kmoser's article "Listening to Your Computer" in issue 41:1. Being able to intuit what a device is doing through the sounds it emits is really useful for troubleshooting. For example, my 2019 Pixelbook Go doesn't include status or activity LEDs, and is passively cooled so it has no moving parts. Therefore, the first sign of life while booting is its relatively loud *coil whine*. I found the sound irritating when I first turned it on, but now it's a useful signal that something is happening when I press the power key before the screen turns on.

Noelle

Dear 2600:

Reading the latest issue (41:2) and "Big Tech Is the New Soviet Union..." This opinion piece I find myself in strong agreement with. Aestetix didn't present any new information, but the rant he went on I found myself feeling that frustration, especially as he talked about how the big tech apologist will say it's their company and they can run it however they want to.

Paul

Dear 2600:

Imagine my surprise to see a photo from Danbury, Connecticut on the back cover (41:2)! That's on me for living near here for ten years and never putting two and two together, but my travels never take me to that part of the city. Kudos to you, PRD, for realizing this sooner.

According to one source (which I'll admit isn't as credible as I'd like, but was all that I could find), the "aunt" was a member of a family with the surname Hack, and she had a bit of a reputation as a local healer. If she really was finding creative ways to use roots and herbs to cure illnesses, one could say that she was a white-hat hacker of her time.

Colin Cogle

Dear 2600:

In 41:1, Oddbjørn sent a letter to inform us that their municipality offers free Wi-Fi through a Fortinet URL filtering system that blocks websites categorized as hacking. As a result, access to 2600.com was restricted. This can be broken down into two aspects:

1) Website categorization by the vendor.

2) Client policy based on such categorization.

The first point pertains to how each vendor offering similar security solutions categorizes a website, usually automatically with crawlers. Whether the label assigned to 2600.com is accurate or not can be debated, but I do not believe this should be the focus. Personally, I would say that "hacking" fairly accurately describes the topics covered on 2600.com.

The real problem here is the municipality's URL filtering policy. Specifically, someone in the company has decided that websites covering hacking topics are deemed dangerous.

There is a genuine belief that sites like 2600.com involve criminal activity, notwithstanding that most vendors offer more appropriate categories such as "malware," "phishing," "illegal," and so forth. This behavior is prevalent in most companies where I have come across similar technologies: investment banking, manufacturing, government departments, and so on.

At the core of the issue is that the mainstream media has managed to distort the concept of what hacking is about, and everyone has followed this dogma without questioning it - even so-called cybersecurity experts. I believe our focus should shift from contacting security vendors to change the categorization of our beloved website to informing news outlets about the proper use of the terms "hackers" and "criminals."

Educating them on this distinction could have a more significant impact.

XCM

The irony here, however, is that our website doesn't contain the information that's in our publication. We have our radio shows, links to our store, information about HOPE conferences and meetings, but not really anything that could be considered controversial. In fact, it's those very media outlets referred to which are filled with stories about hacking, yet somehow they escape the label. It's like we're being blacklisted more for who we are rather than for what can be found on our site.

Dear 2600:

In response to "A Response to a Call to Arms" (41:2), I have been working with Linux professionally since 1996. Every few years, I would install Linux on a laptop to see how the desktop environment was maturing. But I never fully moved off of Windows. I have used every Windows version since 3.0, except ME and 8, up through 11.

When Windows Recall was announced, I decided it was time to migrate. I spent about four weeks testing all of the different flavors. Even though I'm a sysadmin at work, I'm not a Linux god. My personal requirements are basic, to say the least. Browser, GnuCash, LibreOffice, backup software, mp3 player, photo software. I decided to

go with Pop!_OS as I dig Ubuntu but I don't dig Flatpak.

I have now been Windows-free for six weeks. I don't miss it at all.

If friends ask me why I switched, I tell them and I offer to help them. I don't get into flame wars or argue online. I don't have time for it. But from what I saw on forums/websites, there are a lot of people out there who answer questions about Linux with a lot of added nonsense. My favorite is "Why would you want to do that?" Fool, I just want to do it that way, I don't want to have to justify my question. Answer it or move on. Or be nice about it. "That's a great question. Here is how you do that, but here is why you shouldn't."

A big roadblock to desktop Linux is the know-it-all end user who is trying to be "helpful" by telling you why your question or use case is stupid. It can turn people off. I am experienced (old) and ignore that stuff, but new users may not be as thick-skinned.

Just Keep Things Anonymous is absolutely correct when they say "don't get bogged down by other people's opinions on what is the best distribution." Find what is best for you and try it.

Sumo

Excellent points. Being judgmental is never a good way to get someone to see what's preferable about your methods.

Dear 2600:

In 41:2, Jonathan pointed out that Gmail will display another Gmail user's avatar if they have an account. Staff replied that this only applies to people you've previously communicated with.

I can confirm that you can indeed validate the existence of a Gmail account and see its avatar by just drafting an email to them. I just tried using \$ common_first_name_plus_letter@gmail.com, who I've never emailed before, and was greeted by their avatar.

PRD

You are absolutely right. We had tested this, but clearly not extensively enough. What we can't quite figure out is what makes some avatars appear while others don't. We hope someone is clever enough to write a script that will catalog all Gmail users by their avatars. Whether this is a Gmail feature or flaw, people need to know about it. In mistakenly dismissing this, we said it would be a "huge privacy violation" if it existed. Well, it does and it is.

Dear 2600:

In 41:2, aestetix stated that we are allowed to offer criticisms of Google, Apple, and others without risk of expulsion. I would not count on that continuing. I avoid use of these products as much as I can because I realize they can engage in vendor lockout, and I can lose a lot of my stuff because they won't let me have it back. Everything that I have is backed up to services other than those big services so I can make things work.

I recently switched web hosts. Part of that involved transferring email. I would not have had to do that if I used Gmail, but then if Google decided they didn't like something I did, regardless of whether it was for a good reason or not, I'd lose all my email. Everything is backed up offline.

My recommendation to our community is to advise all our friends to avoid vendor lock-in, as it can also lead to vendor lockout.

The piano guy

This is always the risk when trusting a third party. It should be a priority to develop local solutions for consumers. Clouds can dissipate, after all.

Q&A

Dear 2600:

I'm interested in submitting an article to your magazine. I'd like to know what are your specifications for articles (i.e., word count requirements/limits, documentation type, etc.)?

Andrew

We don't have a lot of requirements or limitations. We want people to write about that which interests them for as long as they have something to say and information to share. Some writers cite sources, others are more stream of consciousness. We ask that submissions not already be published and that (obviously) you don't use AI to write your article for you. Those who do won't be taken seriously in the future. articles@2600.com is the address to send your articles to.

Dear 2600:

I recently subscribed to 2600 in paper form, as it was removed by Kindle a while back. I just checked today and noticed they are now again offering the same current 2600 mags on Kindle - Spring 2024 is there for \$5.99. The only thing still missing is the monthly subscription that I had lost before. Can 2600 management verify this?

Peter

You can still get individual issues (not subscriptions) via Kindle, but we should point out that Amazon retains some control over those issues after you've downloaded them. You can pay a dollar less at store.2600.com and "side load" the EPUB version onto your Kindle, where you will be able to have full control over saving and sharing your copy. Simple instructions on how to do this can be found on our main page.

Dear 2600:

Is there any chance of adding *Off The Hook Overtime* into the main *OffThe Hook* RSS list? This would make it so much easier to get the "complete" show for us Internet listeners/downloaders.

Thank you for your consideration.

vhf

This hopefully will be in place and functioning by the time you read this.

Dear 2600:

Hi, I am just wondering if Beavis and Butthead are the only admins on your Facebook page?

manus mcmanus

We'd be honored if they were, but they're very much in demand elsewhere.

We sense you're attempting to create an insult here, but since we have multiple Facebook groups (different from a page which really doesn't need an admin) with multiple admins, we don't really know how to apply it.

Dear 2600:

I was reading the Spring issue of 2600 and saw that "Lee Williams, Harassment Agent" was a work of fiction. Do you guys take fiction? I'm a published author and am working on a science

fiction story I think might be a good fit for 2600 if you do.

I'm also planning on submitting an article I'm working on and am wondering if you guys need any credentials or a cover letter or anything....

curious

It's not nearly so formal. And yes, we do take a limited amount of fiction, which we run as space permits and if we believe the piece fits into the hacker realm.

Dear 2600:

I never asked any of you for a favor. Please can you help me take down nbc.com.

Bruce

Technically you're correct. As you've never asked us for anything before, we are compelled to grant you one favor. You should know, however, that we tend to get these requests whenever the fall schedule begins.

Dear 2600:

Is there any reason to not sell both formats? Right now I get the print magazine (lifetime!) and the annual digests. A quarterly ZIP file with both formats would be nice to have. Nicer: some kind of website where I can go download any of these things if I need to download them again.

matt

We do intend to come up with new packages as soon as we have a moment. Our current downloading system is designed with privacy in mind, which makes it extremely difficult for your data to be compromised when you get a new issue. The tradeoff is that all your info isn't sitting around on our servers, requiring manual intervention to resend lost issues. For now, that seems preferable, as it happens fairly infrequently.

Dear 2600:

I see that you require submissions have not been previously published, but I'm wondering if you have a policy for posting online after they appear in the magazine?

Mike

After an article is published, the author is free to do whatever they wish with it.

Dear 2600:

I am receiving phone calls on my iPhone from my Google Voice number. I haven't answered one yet. I have confirmed that no one else has access to my Google account. In that case, I'm guessing the number is being spoofed, but how would they know to call my cell number with it?

Rob

There are all sorts of possibilities. We don't know if both of these numbers have appeared somewhere online or are part of a profile or even an online order. While a bit spooky, you ought to pick up the next time you get a call from yourself. You may find that it's someone you know who has both numbers and is playing a trick on you, using Caller ID spoofing.

Dear 2600:

We keep getting calls at work that are unwanted and sometimes even harassing. The numbers on the Caller ID are never in service when we try to ring them back. Is there any method available to try and figure out the actual number the call is coming from with the spoofed number? I realize the chance

is probably less than slim.

Paul

Not necessarily. While these calls are likely spoofing Caller ID, it's quite possible that the real data is still being transmitted. We've done experiments with distinctive ringing, where a landline rings differently if a particular number is calling. We noticed that distinctive ringing kicked in even when Caller ID Blocking was invoked. We've also been able to obtain an actual phone number - even when blocked or spoofed - by various combinations of forwarding. For whatever reason, the ANI data is sometimes looked at instead of the Caller ID data, thwarting the attempt to block or mask. We've also had some success forwarding to some cell company voicemail systems. The caller would have to leave a message or hang up after the beep, but they would have no reason to suspect their number was being captured. So "less than slim" is not how you should describe your chances here. There are definitely possibilities.

Dear 2600:

I have a laptop running Linux and a desktop PC running Windows 10. This morning, I watched part of a YouTube video on the laptop. This afternoon, I found the same video using the PC and the video started at exactly the point at which I'd stopped watching on the laptop. Neither the laptop nor PC were signed into YouTube and I have no synching enabled anywhere. In both cases I was using Firefox (again with no synching enabled). I hadn't previously watched the video on the PC. Any idea how this could happen?

David

If both devices are sharing the same Internet connection, it might be possible that the network is caching your YouTube data. YouTube itself could also be using your IP address if you're not signed in, and if that shows up as the same on both machines, it could explain how this happened. More experiments should be performed to see when this does or doesn't happen, such as using a different browser on one of the machines or trying this from different locations.

Meeting Info

Dear 2600:

Looking for meeting location in southwest Arkansas. Thanks.

Aaron

Our current Ft. Smith meeting may be too far north for you, but there's nothing stopping you from starting one in a place like Texarkana (or even Hope!) in the southwestern part of the state. Just follow the guidelines at 2600.com/meetings/guidelines.html.

Dear 2600:

The person who hosted 2600 meetings pre-COVID in Bloomington, Indiana does not plan to start them up again. I would like to start them instead. I found a location, the local public library, with free parking that can accommodate the meetings, however they close at 6 pm on Friday. Is it acceptable to 2600 if we meet there from 5 pm to 6 pm and then optionally hang out in the parking lot afterwards, or do I need to find a new location that can accommodate us for the entire 5 pm to 8 pm time indoors? I have not advertised this locally

yet, but I know there is interest.

Kevin

Many meetings start in one place and then head to another. We think you can do better than a parking lot. But the library is a great start, assuming you're allowed to talk at normal volume in there. Also, it should be noted that meetings aren't "hosted" by any one person or entity, but are a group effort. While one or more people may do the bulk of coordinating and communicating, the meetings belong to everyone attending. We will begin listing this one as soon as we get the specific details.

Dear 2600:

Wondering if you would know if there is any meetings for 2600 in Calgary, Alberta. The last one was in Eau Claire market, but that building was recently torn down....

Robert... in Calgary

We get so many inquiries for this city and also for other cities in Canada, none of which currently have meetings. It's rather bizarre, as Canada used to have so many well-attended meetings. All it takes is for someone to pick a convenient public space and give us the details, while giving us monthly updates.

Dear 2600:

Had a guy that was showing up to meetings for a time. Cool kinda old school hacker, the free speech kind, where it was a place to come together and talk about the world. Been attending, hosting really, the meeting for a while now, and I guess it was a bit of a good thing it took *this* long before I had to ask him to leave, ask anyone to leave, really. And it sucks. But it had to be done. Dude had this habit of bringing physical memes, printed on thermal printer paper, and kinda handing them around. It was cute and novel, in a way. Like an old school kind of hack. Meatspace sucks sometimes, and it is always good to laugh. Til it is at the expense of another. Til you are laughing at the same joke that has caused hate, the same joke that causes death around the world. Then, well I had to say something. It was anti-Semitic. I called it out. Like, called it for what it was, and was met by this gent with "oh, it's just a joke."

There is too much hate in this world. Too many times we just stayed quiet when we might have saved a life by speaking out, speaking up. So I said something. I said it loud, and emotionally, and... I stand by it. Asked him to leave and not come back.

And I feel bad in a way. Anytime that kind of altercation, confrontation, or whatever comes out, it always gives me pause. Am I the asshole? Maybe. Do I feel like I did the right thing, when the alternative would have been worse? Yes.

If more people stood up to casual hate as a form of humor, we might have just a little less hate in this world. If *everyone* did this, it might not be the world we live in today.

wother

While we likely would agree with your assessment, we need to point out that it's not up to one person to decide who stays and who goes at a meeting. If you're in agreement with other regular attendees, this isn't an issue. If not, then you need to talk it through. And please be open to

the possibility that people can mature and change over time, regardless of their age.

Spam & Scams

Dear 2600:

Dear user ID (letters@2600.com)

This is to notify you for the final time that we have stopped processing incoming email and files on your account, since you have refused to upgrade your account to our new service and we will be forced to De-activate your account if this notice is ignored.

Please take a second to secure your account below....

UPDATE HERE

Your security is our primary concern. Regards.

Security Team @2018

Real convincing. You almost had us.

Dear 2600:

Say it ain't so!

Was it something we said?

We can take a hint. You've been distant lately, and we're not sure why. But, we'll always remember the good times we had.

If you no longer want to receive our emails, please click on the button below.

Do we have it all wrong? Do you want to stay friends? Update your email preferences here:

CCMI HUB

This "personal" touch of today's spam is actually more annoying than the generic kind. We wonder if it ever works.

Dear 2600:

We are Anonymous hackers group.

Your site CLUB-MATE.US will be DDoS-ed starting in 36 hours if you don't pay only 0.02 Bitcoins @ [Bitcoin wallet redacted].

Users will not be able to access sites host with you at all.

If you don't pay in next 36 hours, attack will start, your service going down permanently. Price to stop will increase to 1 BTC and will go up 1 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

This is not a joke. Our attacks are extremely powerful - over 1 Tb per second. No cheap protection will help.

Prevent it all with just 0.02 BTC @ [again, redacted].

Do not reply, we will not read. Pay and we will know its you. *And you will never again hear from us!*

Bitcoin is anonymous, nobody will ever know you cooperated.

Anonymous

First off, we no longer have that domain and haven't for some time. Second, this has nothing to do with the decentralized Anonymous hacktivist collective. Third, we fear you may have poor bandwidth as we never received your attack. We can help you upgrade your service - when would be a good time to call?

Hacker Origins

Dear 2600:

So my first experience "hacking" dates back to my single digits. I was a kid determined to find a

way to get Internet as my mother didn't wish to pay a monthly AOL subscription. I played with various dialup numbers and passwords. I gained access to Sprynet at a young nine or ten years old, what I thought was free of charge at the time. I cracked the code... or so I thought. My mother came to me screaming. Caller ID must have tracked the number because we received a per diem bill for well over \$100 (in 1995, this was a lot). I got screamed out for two hours, questioned for another, and ultimately my mom let it go and we never paid the bill. That's my first real "hacking" memory.

Adam

Not to take anything away, but it seems like you may have been the one who got hacked here. Getting people to dial "free" numbers only to have them be billed later was kind of the phone companies' modus operandi back in the day.

Dear 2600:

It was the mid 90s and I was in seventh grade. I was a very unpopular kid who got bullied on a daily basis. Back then, bullying wasn't just kids being mean to me; I was beat up often.

I got sick with mono early into the school year and was home schooled for five months while I recovered. In those five months, I started using our Power Mac and put to use those AOL CDs we got in the mail every month. I started learning HTML so I could build a website on GeoCities for free. What a world we lived in, right?

I realized that all of the kids who bullied me were on AOL as well. Hmmm, how could I leverage this? I noticed that AOL used specific table/frame measurements that limited us on how much text would fit in an email you sent. Because I was learning HTML, I knew I could break this somehow.

One day someone sent me an instant message with graphical smiley faces, and when I received it, my computer slowed down a little bit as it loaded the graphical smiley. That's when I had my idea. I could send a shit ton of smilies to freeze someone's computer. But surely AOL had thought about this and blocked it somehow, probably with the preset size of the table we typed inside of. So I turned off graphical smileys in AOL settings so that when I typed in "" it stayed as text and didn't load a graphical face. I then found the font with the smallest text to use. I then added `<font size=0.1>` and was able to add 300 more smiley faces than AOL ever wanted us to use. So now I would just send an email message with three times the amount of graphical smiley faces AOL ever wanted you to use, putting whoever was on the receiving end of these emails in hell. Oh, and the funny thing about AOL was when you opened it, it would load your emails first thing, so anyone with one of these emails in the email box would be slowed to a crawl, let alone the fact that I sent over 100 email bombs to my victims.

My retaliation towards the bullies worked better than I could ever have imagined. The next week they begged me to stop. A few had their parents call my parents begging them to stop me. They all thought I was cool after that.

This led to my over 20 year love of working in IT. Hacking gave me a voice when I was

physically incapable of standing up for myself. It gave me confidence and it provided me a career that's always in need. I've got so many hacking/phreaking stories from the mid 1990s to the mid 2000s. Nowadays I don't hack for personal gain. I just hack when asked to for my job.

John

Revenge can often be a good motivator for learning about tech. It has to be carefully thought out and it should only be used on those who truly deserve it. Which it sounds like is exactly what happened here. Congrats on making it through Hell.

Dear 2600:

I was just thinking about modems and how I still have them and wouldn't it be fun to hook them up and see if they work. But wait... who would I call? Where can I call and have an actual modem answer? Likewise a fax machine. Then the other problem, I don't have a land line. PacBell is killing them off. Nothing to connect it to. Which brings me to my question. Does anyone make a device that will behave as a POTS line but connects to a cell phone?

Jay

We suggest looking into cellular POTS adapters. But we're more interested in finding out if there are any modems picking up out there. Perhaps we need to start scanning phone exchanges again. (You will still find a number of fax machines.) And fiber should work as a POTS line for those places where copper is being discontinued. But we all know it's never going to be the same.

Dear 2600:

I first learned about 2600 by accident. I was eating at a Wendy's in Rosslyn, Virginia right next to the Court House metro stop (three stops down from the Pentagon). There was a small bookshop/newsstand across the street, so I went over after I finished lunch to see what they had. There was a line of guys from the Pentagon with 2600 magazines in their hands. I asked one of them what was going on. He replied that they were all cybersecurity folks and got the magazine every quarter when it hit the newsstand. I asked why they didn't just subscribe and he replied that they didn't want their names found in any subscriber database that 2600 maintained in case of breach or subpoena.

Bill

It was always a comfort to know that we were making people from the Pentagon nervous.

Dear 2600:

Many years ago, I used to attend an "art college" that had a Mac network with several workstations running programs like Photoshop and QuarkXPress. The network administrators used a program called "At Ease" that would prevent users from running any programs on the disks we used to save our files. (I think they were zip disks?)

I used to take great pleasure frustrating the system admins by easily disabling their "At Ease" security. I found that if I held down the shift key as the computer started, it would disable all extensions (kind of like safe mode for Windows). Then I would move the "At Ease" extension out of the Extensions folder to a temp location and

restart. After rebooting, everything would be back to normal minus that annoying “At Ease” software. I would, of course, move it back into the extensions folder so that when it rebooted, all would be back to normal.

Then I could run any software I wanted. It drove them mad and they had no idea how I was doing it.

Mike

Until now when hopefully one of them picks up this issue.

Concerns

Dear 2600:

Since I saw you accept cryptocurrency, I was interested in buying all the back issues and a lifetime subscription. It was going to be awesome, but then took the most dystopian turn imaginable. Let me walk you through my experience.

I get a CAPTCHA before I could visit the store just because I use privacy software. Not what I expected from a hacker mag, but whatever, I can do a CAPTCHA to get to the store to support you.

Unable to place the item in my cart. Normally, I'd just bail at this point, but I really want to give you money, so I try again without Tor browser and no CAPTCHA and the cart works fine.

I put the item in the cart and attempt to check out using Coinbase. It says there was an error with the payment processor. No indication as to what the error was, but okay, there's another crypto checkout option, so I selected BitPay. No big deal.

They want me to register for an account. Ugh. But you know what, I'm willing to sign up for yet another account just to make this purchase.

So far it's been a long string of annoyances, but this is where the story takes a radical turn. In order to pay, I need to:

1. Provide my biometric data: face scans and voice recording.
2. Consent to have this information disclosed to others and re-disclosed.
3. Hand over a photo ID, which will be shared with third parties.
4. Disclose my location, IP address, and “other device data.”
5. Consent to six months of “processing” all of this data, and allow them to store it for one to three years.

I have so many questions right now, but I can distill them down to these three:

A. Were you aware you were doing business with a company who was asking this of your customers?

B. Do you feel these are reasonable steps that people trying to subscribe should go through?

C. Can I just send you money and you send me a box of magazines and put me in your database as a lifetime subscriber?

I feel like the transaction should go more like this:

Me: Yo, I want all back issues and a lifetime subscription mailed to XYZ. I'll pay in ETH.

You: Send 0.204 ETH to SomeWalletAddress.

Me: Done.

You: Shipment should arrive in a week or two.

Me: Pleasure doing business with you.

You: Likewise!

At any rate, despite this experience, I *still* want to support your work, but there's no sodding way

I'm agreeing to these terms. I hope we can reach a mutually acceptable solution to this problem.

Thanks.

Adam

We appreciate your persistence and documentation. Absolutely none of the above is done at our behest, but appears to be a symptom of the current cryptocurrency culture. There's a limit to how much time we can spend tweaking these methods so that they work in a variety of scenarios, so we go with what's made available by the companies we already have relationships with, such as Shopify, BitPay, etc. Even then, we are constantly barraged with changes from their end which we must work through, as well as tools that inevitably break because of changes they implement. We are always open to trying out new methods, but they need to be able to play nice with the existing services we use. That doesn't always happen.

While we love the concept of cryptocurrency, some of the privacy issues involved are extremely concerning, as documented above. Clearly, there's a bit of maturing that still has to be gone through, so it's going to be a bit of a rodeo for some time to come. We're certainly willing to consider alternatives, but oftentimes the hoops we're told to jump through are as unacceptable as the ones you cite above.

And yes, you can always just use old-fashioned postal mail for any of this.

Dear 2600:

Another symptom of corporate control: I have an Android phone. I simply want to play my mp3s. I also happen to have Spotify. No matter what settings I wrangle with, the phone mandates I use Spotify to play my local files. I *cannot* simply play mp3s without it. I tried getting other apps, no luck. I just gave up. Now this would be bad enough, the idea we're getting herded into subscriptions. But it gets worse... Spotify is horrible for playing local files. It gets confused if you rewind or switch songs. *Wait* - it gets worse.... I'm a vain musician with brain damage, so there were mixes I'd play over and over (away from family, don't worry) and consistently, after enough repetitions, Spotify would eventually *not allow* me access to the files.

So let me get this straight... I *have* to use your paid-for app to play *my* local files... but only until you say so. Sorry for the non-hacker ramble, but seriously. Seriously.

Daniel

This can't be right. We don't use Spotify primarily due to the shitty way they treat musicians whose music they profit off of. But if this were truly how it operated, we would be sure to delete it off of our phones right away. There are many alternatives and Spotify is not essential for hearing music. We would like to hear from musicians who have found other tools that work better for the user - and for the content creators.

Dear 2600:

My ophthalmologist (that's a fancy eye doctor for old farts like me) sees a few dozen patients a day in this grossly under-served region. You can expect to wait three to four hours *with* an appointment. But I digress.

Sitting in his examination chair alone while he saw the patient in another room, I chanced to look at his computer monitor which faces the exam chair. There was the record of the previous patient for me to examine or worse, without restriction of any kind.

Even worse, there was a well-yellowed computer-printed file folder label stuck "permanently" to the monitor, proclaiming "[Such-and-such] System, password: Newpass123".

So many levels.... Just goes to show that making five figures a day doesn't necessarily mean you have any smarts about security.

Tau_Zer0

We doubt your ophthalmologist makes \$2.6 million a year, but that's not the point. The waiting time seems a bit unbelievable, too. Again, not the point.

This kind of thing is more common than we'd like to believe, unfortunately. When it happens, we advise getting a quick picture and leaking it to a local newspaper. (Be sure to avoid any timestamp either in the picture or the metadata.) That is, assuming you don't think pointing it out would do any good - we know many times the messenger is treated as the culprit when revealing security lapses.

Dear 2600:

The so-called Five Eyes Agreement, which is a treaty between the countries of United States, Canada, New Zealand, Australia, and United Kingdom that has been in place since the 1940s, should be abolished. The Five Eyes Agreement between these countries is a violation of each of their citizens' right to privacy by intercepting their communications of various sorts including email, telephone, Internet, and fax through a program called Echelon Surveillance Network without having a warrant to do so, even though some will argue the threshold for requiring one varies from place to place. The other issue with the Five Eyes Agreement concerns listening posts that are stationed in other lands, such as Menwith Hill (U.K.) or Pine Gap (Australia) to name a couple. Citizens didn't okay having a foreign entity based in their country. The Five Eyes Agreement paved the way for mass surveillance of not only domestic communications of citizens but another country's as well. This should never have been given the green light to do so for the above reasons, plus the fact that there's little to no oversight or transparency.

Bill

The lack of oversight and transparency is precisely what is appealing to intelligence agencies. Fun facts: there are also groups known as Nine Eyes and Fourteen Eyes; Five Eyes members promise not to spy on other members' governments but have no problem spying on other members' citizens; and the five English-speaking member nations are also referred to as the Core Anglosphere.

Info

Dear 2600:

Are you Canadian? Are you mistakenly angry at the Canadian government for censorship? Shouldn't you find a way around this drama?

Follow these steps to reduce your stress, and keep Facebook from preventing you from posting news articles: 1. Copy the link of the news article you wish to plague others with; 2. Go to wayback-api.archive.org/; 3. Post your link into the Wayback Machine; 4. If the link is already archived, copy it from the web archive; 5. Paste that to Facebook, post it, and stick it to the man/people!

Corey

While people shouldn't have to resort to this, it's important to understand why it's happening and not simply buy into what Meta (owner of Facebook and Instagram) is saying.

If you try to post a link to a news story in Facebook or Instagram, you'll get a message saying "In response to Canadian government legislation, news content can't be shared." Since they're the ones controlling the message, the natural instinct is to blame Canada. But it's not so black and white.

The Online News Act went into affect in 2023, requiring Meta to pay for the news content it displayed on or through its site. Google has already reached an agreement to pay approximately \$100 CAD annually to Canadian news outlets. Meta claims its users don't benefit from displaying or linking to news, a claim its users might disagree with. Meta reacted by cutting off all access to Canadian news sites rather than pay, in all likelihood concerned over the precedent this will set in other countries.

But there's one fact that's not so easy to evade. Journalism has been taking a hit worldwide and advertising dollars have plummeted at newspapers, magazines, and TV/radio news outlets. Meanwhile, social media giants have been making record profits from advertising. It's not going out on a limb to suggest there's a connection and that something needs to be done to even things out.

We've all seen what happens when people get their news purely from social media, i.e., not from accredited news sources. Old style media should certainly be challenged and other perspectives should thrive. That doesn't mean no standards at all or that pretty much anything goes, as we've seen recently on many social media sites.

Dear 2600:

My class "predicts" that "singularity" - that point where AI has the same level of intelligence as humans - will occur by 2045. I assure you, I know of at least one system that has already achieved it.

Marcus

And you couldn't add one more sentence to tell us which one?

HOPE XV Feedback

(Note: These letters were sent as feedback for this summer's HOPE XV conference and, as is our tradition, we thought they would be of interest to readers. Since we didn't explicitly tell writers that these comments might be printed, we have omitted names.)

Dear 2600:

This was my first time attending HOPE. I've been reading 2600 for years and so I was aware of the conference, but never thought I'd have the chance. But this year I attended virtually. Just wanted to say thanks! Everything went smoothly

on my end - a few A/V bobbles in some of the rooms, but people would report it quickly and it always got cleared up. Otherwise, it was great! So many great talks. Keep up the good work!

HOPE XV Attendee #1

This year we did a lot more with house A/V and we believe it worked for the most part. But there will always be issues, especially the first time a particular configuration is used. We think we've got a really good foundation to build upon in the years ahead.

Dear 2600:

Some things that would help for talks would be captions (even auto-generated captions are helpful, if imperfect), reminders to speakers to repeat questions before answering/ensuring microphones are available for questions, and ensuring that video allows for lip reading during speaking portions.

HOPE XV Attendee #2

All good suggestions that we will continue to work on in future conferences. These things become possible when people step up to help with our challenging A/V needs.

Dear 2600:

This is my feedback after attending HOPE for the first time - what I'm calling my zeroth HOPE. I had an incredible time and wondered why I hadn't participated before. The dedication and hard work of organizing this event are truly commendable.

The food trucks were a fantastic addition, especially since I heard food options were minimal over the weekend. However, I had a vegetarian friend with me, and unfortunately, neither of the food trucks could accommodate vegetarian options. In the future, it would be great to see more inclusive food choices, including vegetarian and vegan options.

I also loved the bustling atmosphere in the vendor and village area. I heard from one of the vendors that, at the last HOPE, the vendors were placed elsewhere apart from the rest, resulting in long periods with little traffic. Although I can't compare it from personal experience, having everything centralized - the vendors, registration desk, info desk, and villages - seemed like a smart move that significantly added to the lively environment and made the event more enjoyable for everyone.

One other piece of feedback concerns the Little Theatre. At some point, the handrails became sticky and unpleasant. It was probably due to something spilled or the varnish wearing off, but it was gross, and I avoided touching them for the rest of the conference. I also found that, after going into the restroom at Little Theatre to wash my hands of the sticky stuff, the bathroom was out of soap.

Overall, my first HOPE experience was terrific, and I deeply appreciate all the effort that went into making it happen. I'm eagerly looking forward to attending again!

HOPE XV Attendee #3

Nearly all of the changes for this conference came about as a result of feedback from the last one two years ago. We moved to a different location on campus, as a number of people weren't thrilled having to walk up a hill each day. The new buildings not only solved that issue, but allowed us

to place vendors in a more heavily trafficked area. We believe the waffle truck had both vegan and vegetarian options. The other truck specifically told us they would have those options and then showed up with only burgers and fries, so we won't be using them again. Overall, the concept worked well and we will continue exploring our options.

Dear 2600:

Thanks for a great conference - having the virtual option allowed me to experience the HOPE culture and community from Australia, and to spread it around locally.

I can't recall if I selected the option to get a badge when I booked my ticket, but I don't see any mention of it in the emails from you or 2600 so perhaps not. If you do still have any left, I'd be happy to purchase one. I also heard about t-shirts and I think a printed program or other swag being available. If there are any left over, I'd be grateful to receive some of those as well. I'm happy to cover the costs of any items as well as shipping, of course. Just let me know if there's anything available.

Congrats on running a great conference, I'll be back in 2026 if you continue offering virtual tickets.

HOPE XV Attendee #4

Our virtual audience expanded quite a bit since last time and we've heard a lot of good things from them. You should have been contacted concerning receiving our laminated badges. (We're not able to send out any of the electronic badges that were donated, as those only covered in-person attendees.) We completely ran out of printed programs this year (which proved to be quite popular). And if there are any shirts left, they're only available in a couple of sizes at store.2600.com.

Dear 2600:

So I didn't attend in person and I then forgot to buy my online attendance ticket. Then I was really happy to find out that the talks were all streamed anyway! Which is cool (thank you) so now I'd like to send a donation equivalent to the cost of the online ticket but I can't find a "donate" button on your site. (I bet it's obvious and I'm just being screen blind.) So can you let me know how to do that please?

Hope to sign up properly next time - thanks to everyone who put it all together.

HOPE XV Attendee #5

It's true that we stream the talks, but the virtual attendees are able to interact with others and ask questions of the speakers, which is why that option has become so popular. As for donating, we always prefer to give something back. You're welcome to buy something at our store and, if you truly don't want anything in return, just tell us not to bother fulfilling it. But we really prefer to always send something.

Dear 2600:

Just wanted to say that the remote experience was amazing.

The streams all worked the first time and they weren't locked to some weird format, so I could stream them to my TV and expose the family to some of the Big Thinkers, like Cory Doctorow, Jeff Man, and the other old farts. And your talk

selection was awesome. It wasn't all old farts like me: there were folks with totally new tech and the Enthusiasm Of Youth. The Matrix was flawless, very usable, and super helpful. (That's where I got the idea to email!)

The tech was awesome, the talks were awesome, the people were awesome, I'm completely coming to New York in 2026! Save me a seat!

HOPE XV Attendee #6

We look forward to it.

Dear 2600:

Thank you for putting this event together! My one bit of feedback is on Matrix access. I bought a ticket at the door on Saturday, and because of this, never found out that I was supposed to get a token for access to a Matrix space (I found this out on the wiki, unless it's outdated). It'd be great if there would be an alternate way to access the Matrix space next event.

HOPE XV Attendee #7

This was an oversight on our part which affected those who bought tickets at the event. It likely happened because this was the first time we sold tickets in-person since 2018, but that's no excuse. We apologize to anyone affected. If you still want to join (since the various channels still exist), we can send you a Matrix code.

Dear 2600:

Thanks for the amazing conference. I was able to grab m3u8 URLs from livestream.com and view all three tracks with ffplay. I fed this into my transmitter and broadcast the first two days of HOPE on VHF channel 13 (I originally wanted to use the mystical channel 6). Slides were visible and mostly readable, even at what is practically VGA resolution (minus overscan).

Now for my criticisms on HOPE's streaming. The biggest problem was that the livestream's m3u8 URL would periodically change. Then, I would have to go off-air and grab the new URLs every couple of hours. Very problematic for broadcasting overnight and as a one man band! I expected after all the commotion with YouTube, direct streaming URLs would be published on the HOPE website/wiki as I said previously. Instead I had to rip them from the streaming site itself. I feel like this is something that could easily be done, but wasn't despite the demand. Having direct, static URLs for each track available should have solved the problem of me going off-air.

Overall, great conference! I look forward to attending the next one in-person.

HOPE XV Attendee #8

We're not entirely sure what it was you were doing or where. But apparently HOPE was being broadcast over the air somewhere, which is fine with us but not really what we're set up for. Our primary goal is to make sure physical and virtual attendees were able to have access to what they wanted and we believe that is what happened.

Dear 2600:

Thank you for putting on an absolutely amazing conference! It was my first HOPE and I loved it!

I quickly realized that the three main talk tracks were being livestreamed/recorded and would be available to watch afterwards, so I attended all the workshops I could and had tons of fun learning

about Arduino, ESP32, Lilygo, and building colorful blinking LEDs, LoRa terrestrial and satellite transceivers, a TV-B-Gone, and an audio distortion maker.

Tonight I found the talks on the ISOC-NY livestream.com page and I've been watching hours of it already. Thank you! This is wonderful!

Unfortunately, there are a few places where the stream freezes during the talk. This is not my connection, but a problem with the cloud recording.

My feedback is that it would be really great if the livestream and recordings are improved for the next HOPE.

Thanks again for an awesome conference!

HOPE XV Attendee #9

We believe these problems have been fixed with our local copies which should now be available online and physically. Nearly every technical problem we had could be fixed with more people helping. Some of our staff, though thrilled at the success, were incredibly overworked.

Dear 2600:

HOPE XV was my second HOPE, having previously attended in 2022. So I'm coming at this from the perspective of someone who never made it to the Hotel Penn (RIP).

I had a great time! There was a great selection of talks and I enjoyed several of them. Most memorable were Mitch Altman's community talk, Dan Romanchik's ham radio talk, and the Library Freedom Project panel. I saw someone online refer to HOPE as "the arts and humanities hacker con" and I like that description. Rather than being purely technical, the diversity of talks and attendees makes HOPE a unique experience. I even recommended it to non-hacker friends who have interests adjacent to HOPE's, so maybe you'll get some new attendees next time.

I also volunteered for the first time this year, as a security person. The other volunteers I worked with were all very friendly and approachable, and welcoming of a first-timer such as myself. I also had occasion to interact with Operation Hammond as part of this role, and they're a great group that adds something important to HOPE. I hope they'll keep coming back.

I stayed on campus. The multiple walks across campus in the sweltering heat weren't great, but no one can do anything about that. The value for money couldn't be beat. I would suggest to the St. John's conference staff that the 11 am checkout time be made more explicit at check-in. I didn't find out until well after 11 am on Sunday, but the St. John's staff was still able to take care of me.

The food, via both St. John's and the food trucks, was good. I got to taste Club-Mate for the first time. (My opinion is still being formed.) I also met up with a local friend of mine and had some excellent biryani (albeit well off campus, in Jackson Heights).

I have no particular criticisms of the HOPE event, staff, or volunteers. Everything went well for me and I wouldn't change much of anything. Overall, I agree with the consensus that HOPE XV was the best yet. I look forward to returning for HOPE XVI, and to volunteering again.

Thanks to all who made this happen.

HOPE XV Attendee #10

Of course, we must thank our attendees, because without them, none of this can happen. We also want to thank the St. John's staff and community, along with ferrymen.net for their donation of Club-Mate for our attendees.

Dear 2600:

I can't believe what you all have done. I've been to a handful of HOPEs at the hotel, the COVID HOPE, and the first one at St. John's. This time, having bought a ticket with the intention to attend, I could not (surprise stomach virus, block *that* AVG!), but I watched much of it on the stream, including the closing ceremonies, which helped describe for me what it was like to be there in person.

And holy shit, I can't believe what's happened here in the span of two years. The parking, the food, the A/V, the livestreaming! I remember hearing there were YouTube problems with the streaming last time; oh my god, how easy was it to look up a talk, and with two friggin clicks, be watching that talk in real time (and no ads!).

I found St. John's to be a bit of a food desert last time, and taking place in the summer, found it not impossible but highly uncomfortable to walk to the restaurants off-campus. Well, I heard in the closing ceremonies that you coordinated with the University cafeteria and made a special menu! Get the hell outta here.

The parking also - I drive from New Jersey, and remember parking in a deck that was a long walk away from the venues, and again it was so hot that I dreaded the walk to and from my car each day. But I heard in the closing ceremonies that you coordinated with the University to get us access to the "general parking" closer to the venues. You all have been working hard these past two years.

There were like 100 talks - the depth and breadth was awe-inspiring. I spent one entire hour listening to an emergency response firefighter talk about how to use a car's computer to help save the lives of car crash victims, one hour about how the porn industry isn't covered under Europe's Digital Services Act (DSA) even though it obviously falls under their definition of a "very large online platform," and one absolutely Club-Mate-fueled hour from a former prison inmate about the multifarious surveillance apparatus of the prison industrial complex. That was only three of the 100 talks, and that's not even including the workshops and late night performances.

Even the Club-Mate - I didn't remember seeing it at the last conference, the first one at St. John's, and I was sad, like it might be a sign that this whole thing wasn't gonna work.

Man, was I wrong. I didn't even go and I had a great time.

Thank you so much to all the people who make this happen, but most importantly for literally keeping HOPE alive - there is no more question about it - the Hotel Pennsylvania is gone, but HOPE will live forever.

HOPE XV Attendee #11

That's a really good summation and assessment. And it's great to see that virtual attendees felt so much a part of everything. Again, all credit to the

attendees, volunteers, and staff at St. John's.

Dear 2600:

Thanks for taking feedback on the most recent HOPE convention. I have zero criticisms about this year's con.

The change of buildings from 2022 was *most* appreciated, and the buildings selected were the perfect ones.

Little Theatre is charming as heck. Tobin and its classroom-ness fit well the workshops. The air conditioning there was *amazing*!

Marillac, though, was the place that really brought this all together; that communal space and all its opportunity for interaction, the cafeteria (another communal function), the vendors weren't just there to sell you something - they were teaching you something, showing you, talking to you.

It was community. Loved that!

To the college cafeteria staff, pass on a very hearty thanks! Good food, decent prices, patient folks.

And yes, those food trucks were the whipped cream on the whole Belgian waffle!

I have a suggestion and a "wouldn't it be cool if..."

Suggestion: shuttle back to the HOPE hotels and/or off campus housing after 12:30 am when the Q30 stops running.

"Wouldn't it be cool if..." you somehow did a shuttle or something once a day to the Tesla lab. Don't know how that'd go down, whether it's something folks pay for, or a part of a package when you buy a ticket... somehow include an additional donation to the lab project? Maybe. I don't know.

Wrapping up here: the volunteer staff I got to work with were fucking great! I thank everyone for their patience, and feel fortunate to have the pleasure of working with so many cool people. No uptight BS. Everything reet. I'd love to come back again, if you'd have me.

Thank you - everyone! HOPE XV was a favorite experience of mine.

Let's do it again sometime.

HOPE XV Attendee #12

Thanks for the kind words. Buses actually run around the clock, though not as frequently as during the day (and not the Q30). But we can look into having a vehicle on standby for people who need a ride to the hotels. It would involve some coordination, but it doesn't seem to be too much of a hurdle.

A shuttle to the Tesla Wardencllyffe site, however, would basically be a day trip as it's 60 miles away. That seems like an endeavor for a non-HOPE weekend or perhaps the day after HOPE.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99,
Middle Island, NY 11953 USA

Effecting Digital Freedom

by Daly Barnett

Paternalistic Age Verification Mandates Are Out To Get Us

If you've been paying attention to tech news, you know all too well the surge of "Protect the Children" bills that are popping up all over the place. You probably know the type: the Internet is corrupting the minds of the youth, privacy shouldn't extend to everyone because that means bad people too, and the entirety of the Internet should have its sharper edges filed down because kids... blah blah blah.

These types of bills must die before they pass. Sometimes they seek to undermine encryption. Other times the end goal is to restrict the constitutional rights to free expression. Any side effects of outsized negative impacts on marginalized peoples, stifling innovation, and chilling politically dissident expression, are - according to proponents of these terrible bills - necessary for the ultimate goal of "Protecting The Children." The latest promised tech solution for these paternalistic goals is age verification.

Age-validating tech schemes come in a variety of terrible flavors, none of them worth the time it takes to learn about them. Some age verification relies on users uploading a government document alongside a real time snapshot of their face. Another method, called "estimation," tries to guess the user's age based on various biometric data or context clues like a user's direct message speech patterns, subscribed interests, and the like.

The failures of the top vendors offering these services tend to fall along racialized and gendered lines. A NIST study published in 2024 shows that the top age estimation and verification vendors haven't improved in accuracy since they were last surveyed in 2014. They tend to age Black people older than they are and Asian people younger. Unsurprisingly, the greatest level of accuracy is found estimating the ages of white people.

The notoriously disingenuous company Thorn (big proponents for the extremely stupid and detrimental Internet legislation FOSTA-SESTA) market the other type of estimation scheme mentioned above: using context clues. Their claim to accurately guess somebody's age based on the content of their social media messages would be novel and impressive if they were true, but Thorn has a reputation for hyperbole. For a refresher on their history of fudging numbers and profiting off creative bookkeeping procedures, check out Violet Blue's damning Internet article, "Sex, Lies and Surveillance: Something's Wrong with the War on Sex Trafficking." Regardless, their current claim about context-driven age estimation makes some bold and dangerously naive assumptions about the speech and behavior of people based on their age.

Speaking of companies conveniently positioning themselves as providers of the necessary products for bad Internet regulations, Google Chrome is now launching its own take on age verification: the Digital Credential API. Exactly how this will be used by websites is still unclear, but the API is available for testing now, which provides a few helpful data points that services can query about a given user:

family name, given names, birth date, portrait, and age over 21. Do you really think that Chrome - a browser built by an advertising company with such a twisted reputation for invading user privacy and dark patterning consent through shady marketing tactics (*ahem*, Chrome's so-called "Privacy Sandbox"), that also just so happens to be developed by the same company that makes the most common third-party tracking mechanisms across the entire Internet - can be trusted with such information?

Even if it wasn't such a privacy and security nightmare to essentially have your government-issued ID living inside your browser for any website to look at, do you think, in your hacker heart of hearts, that the system itself would be able to identify every unique user and follow through the mythical security-tight way of verifying their age? How would that be determined? Their IP? The user agent? Some heinous browser fingerprinting correlated across some other context clues? Would each unique installation of a browser on a device assume that it's owned by only one unique person in the world?

The reality is, even if the age verification systems proposed were truly secure and private (they are not, they will not be), the proposition itself is entirely gameable.

Something like 20-odd states have some sort of Digital ID system in place right now. You might worry that the failures of these technologies described above would create the necessary conditions for a federal mandate on Digital ID, which would then feed into whatever age verification rule is blanketed over the Internet. Don't be surprised if this becomes the next argument in this slapstick routine of garbage Internet bills.

Besides the fact that such a national digital ID system would further oppress undocumented people, people living in poverty, people who've navigated name changes, and more, it's a naive assumption that the Internet is constructed in a way that could support such sensitive information in a secure manner. The Internet is a shambling horde of duct tape and scar tissue. Relics of antique vulnerabilities long since patched live on in bizarre HTTP headers. Automatic code updates can cripple entire industries. Vulnerabilities continue to be found in the stupidest of places. Assuming that the browser is a safe place to store such sensitive personally identifiable information, even with whatever theoretically compelling triangulation of verification schemes they try to sell us on, it's a foolish idea. And if you're buying it, we've got news: there's a pool on the roof, and all your friends are waiting for you.

So, what can you do? It's important that you let your local politicians know that this won't fly. Proponents of these bills are counting on the idea that people are too ignorant of how the Internet truly works to oppose them. Head to act.eff.org to see all the bills EFF is fighting against (or in some cases, even pushing for). And if engaging with politicians isn't your thing, that's fine, we'll do it for you. Our donation page is also at eff.org/no.

Memories of a 30-Year-Old Non-coding Hacker

by Nico Andrews

I was born in 1994, which means that I recently turned the same age that my father turned only three hours prior to a whole new century beginning and three whole hours before the Pacific time zone awaited the world-ending change of the computer clocks. I was five years old then and, at that point in my life, I struggled to understand why the kindergarten teacher changed all four-year digits on the wall when we returned to class. I also struggled to understand why I had to adhere to the arbitrary rule of capitalizing the first letter of my own first name.

One thing I wasn't struggling with was pointing and clicking around my dad's Hewlett Packard Pentium II PC running either Windows 95 or 98 and likely less than 128 megabytes of RAM. We had three games that my dad allowed my older sister and me to play on the computer: *Red Baron*, Megagames (a shareware sampler), and eventually, Humongous Entertainment Games' *Pajama Sam: No Need to Hide When It's Dark Outside*.

My father explained that any of the games contained on the Megagames CD-ROM required that I doubleclick the .exe files in the Windows Explorer. This dumbfounded me, as the images on the CD-ROM case showed an easily browsable menu which definitely didn't coincide with what he was telling me. I only recently rediscovered the CD-ROM in a box in his garage (but no HP Pentium II unfortunately), and learned that the CD-ROM was actually meant for DOS. At some point, within six months to a year on either end of the memory of watching my dad turn 30 three hours before the Y2K bug was set to cause a world meltdown, I remember falling asleep under one side of his large corner desk while he AIMed with his longtime friend using a 2400 baud connection and memorizing the sound of the dial-up modem connecting to the AOL networks eventually resulting in a "You've got mail" audio prompt through the speakers. I was fortunate to have a father who got his undergraduate degree from UC Berkeley in the early 1990s, as I don't think that he would have seen the value or worth in the technology otherwise. I recognize that my siblings and I are lucky that he always found a way not only to afford a home/family PC, but also a connection to the Internet all throughout my life. I myself in my middle school years would

heavily utilize AIM to chat with my friends even if my Internet connection no longer relied upon AOL dial-up connections.

I miss Windows XP and I am nostalgic for those days of playing *RuneScape*, *Age of Empires*, or *The Sims 1* and *2*; learning to rip audio CDs and make my own custom mixes; as well as waiting all night for Limewire or Kazaa to download entire CD albums, only for each song to be either just a song sample, a Rickroll, or Bill Clinton's famous clip about Monica Lewinsky. Only once I learned about Ubuntu Linux in 2008 did I realize the full potential of what a computer could do.

All throughout my time in public school, I was exposed to systems of all kinds, whether it was learning to type from Mavis Beacon on Windows ME computers or *Oregon Trail* in a lab full of old yellowed Apple Macintosh computers. My middle school had both Mac and Windows computer labs. The Mac lab was full of slimline iMacs, the sample music for which included Nirvana's "Rape Me" on iTunes. I learned about the backdoor Windows XP Pro Admin account that could be accessed by pressing Ctrl+Alt+Del at the login screen on school computers, which enabled me to run programs that I wanted to run (and on one particular school computer to create my own admin account on that particular workstation). Eventually, I was running my own apps and Linux distros off a USB flash drive.

At home, the family computer was upgraded to a Gateway desktop with its infamous cow patterned color schemes and designs and, at one point, I accidentally lost all the family photos thinking I was partitioning a dual boot Ubuntu Windows XP system. When one of my uncles moved in with us after experiencing a mental breakdown and subsequent divorce, he used a part of his work disability settlement payout on computer parts and, for the first time in my life, I learned how to properly build a computer part by part - and enjoyed top of the line gaming on a big screen TV at that.

I wasn't ever gifted or able to purchase any of the latest tech growing up, but I was fortunate to have cousins and friends who would give me their one-year-old devices to jailbreak or tinker with on my own, whether they were an iPod Touch or the original Sony PSP. These various tech acquisitions from friends and family allowed me to sell various random old

computer parts for a one-way ticket to the town where I would be attending college.

In my college years, I grew less enchanted with Windows system “upgrades” after the Windows 8 drastic UI change (I tolerated it and for a solid moment embraced it, only to realize how terrible it actually had been upon Windows 10 being released). Having a little bit of my own money working a job at a pizza restaurant, I was able to afford paying for apps and online purchases for the first time in my life and not rely on torrents.

I recently felt saddened at the idea that software, especially that which allows for the electronic creation of art and media - ahem Adobe - would forever be bound to monthly or yearly extortion subscription payments and that physical media would become a hobby for collectors and not those who might truly appreciate the software for all it can/could do. James Bridle offered me some commiseration about this notion in his recent book *New Dark Age: Technology and the End of the Future* where he describes in one chapter the idea that true innovation due to hardware or software limitations has ceased to increase at the rate it once did due to Moore’s fLaw [sic].

While computer building remains to be a big part of PC culture, I sense a shift in its essence as it becomes clearer that specialization of computer hardware in the same way that once existed in the early 1990s and 2000s is becoming increasingly rare. Gone are the days of quirky ideas and, increasingly, only that which can be commodified into a micro-transactional subscription-based model survives. Those who are growing up in today’s world may never know what it was like to pirate share software and media as those of my generation did, nor will they have the same amount of fun in browsing retail store racks for random never-heard-of third party peripherals and accessories in the same way. The subreddit r/PCMasterRace will indicate as much if you spend any time in the comments of posts made since the start of the pandemic.

More and more, I see headlines lamenting the idea that high schoolers who graduated between 2016 and 2024 are entering the workforce with less and less basic computer literacy, possibly due to Chromebooks obscuring even further a basic understanding of computer files and file structures. The examples cited range from social media - Chinese-owned or not - serving as a repository of videos that many Gen Zs are perfectly comfortable using as their photo and video backups instead of paying for storage.

I sense that this obfuscation of data structures and ownership to the end user is intentional on the part of big tech regardless of malintent. I also sense that despite the claims that youths of today will never know the struggle of just how slow HDDs were or just how incredible it is that a small flash drive in 2024 can hold as many as 728,177 3.5 inch floppy disks, they are in fact finding other ways of hacking tech, but at a cost that generations past never necessarily realized. Google Drive may have created a generation of kids who don’t know what a PDF is, but it also created a generation of kids who utilize that same system to send their friends copies of college textbooks that cost way too much on top of exorbitant tuition on top of the highest costs of housing ever experienced in American history. My YouTube feed has recently been playing videos uploaded in 2024 that have a very 2001 visual quality to it. I suspect it has more to do with the webcam quality of Chromebook the person has owned since their high school or middle school days - and still the song or cover they uploaded is lit.

I still try to upgrade and max out the internals of the computers in my life, including the annoyingly difficult to upgrade iMac of 2019 that my partner purchased on Facebook Marketplace. I dual boot Windows 11 alongside Kali Linux - ironically on an HP laptop purchased in 2022 - and run my own personal Linux cloud server for my iPhone photo backups because I don’t trust that Google or Apple won’t expose my images to some third party, or worse, utilize my photos for training harmful AI programs for nefarious non-ethical actors around the world. Some folks might not consider anything I have offered here to be “hacking” in its traditional sense, I know. But there’s more to hacking than simply laboring to find an exploit buried in lines of code or in some hardware architecture for unlocking the true power of physical devices and processors. There is a communal spirit in hacking that still exists if you go in search of it. RaspberryPi, Arduino, and many other similar groups/companies/organizations are just a few efforts which, at their core, bridge gaps between people of different spacetimes - and 2600 is one medium for connection between spacetimes as well. The shared mutual belief in collaboration despite limitations inherent with any electronic device or application or system indicates (at least to me anyways) that communities which foster the hacking spirit can and will continue to provide for generations to come.

How Ubuntu Helped Me Escape a Cult

by NaNaSHi

I am brand new to the 2600 community, and have attended only one meeting so far. However, it is clear to me that I have finally found my people, as I feel right at home and have already made some new friends. I want to tell you all my story (or at least some of it).

I grew up in what I consider to be a cult, and what others would call a sect of ultra-Orthodox Judasim. In my community, we had a lot of rules for everything we did throughout our day. We had rules about what we could eat, rules about what shoelace gets tied first, rules about how to wash your hands after you leave the bathroom. We were not permitted to associate with outsiders, or even with other Jews who were considered “less religious.” Breaking any of the rules would earn us punishment, and those who left the community were ostracized and treated as if they were dead.

The rabbis who made the rules that we all followed had a lot of pet peeves. Certain “issues of the day,” if you will, might include the length of high school girls’ skirts, whether or not it was permissible to attend a college, or the length of time one must wash strawberries in soapy water in order to render them kosher. One of these pet peeves was the terrible, horrible, secular Internet.

The Internet was a place of filth and ritual impurity. The worst heresies in the world could be found online, and the seduction of adult videos was like having “a pocket *zonah* (prostitute).” The Internet was such a corrosive influence and “emergency for our pure children” that the rabbis organized several high-profile *asifas* (conventions) against the Internet. One of these took place in rented-out Citi Field, and ironically can be viewed on YouTube. Thousands upon thousands of cult members paid good money for seats in order to hear the aging European rabbi rally against “the horrors today’s youth face.”

The Internet was becoming increasingly necessary in the modern world, however. So the rabbis came up with a solution. We would have to get filters to block inappropriate websites!!! All the religious schools, gatekeepers of the religious community, enforced the installation of web filters on student devices. Students caught using unfiltered Internet could face consequences and even expulsion. Parents would sign contracts with the schools, affirming that they complied with the filter rules, and that all devices in their household had filtered Internet. Devices would be checked and given seals of approval.

On paper, this doesn’t sound so terrible. Porn is not great for teenagers, after all. But the filters blocked much more than just porn, and they weren’t just for the teenagers. The filters blocked Google Images. They blocked YouTube. Some of

them blocked Wikipedia. Information was tightly controlled, and everyone in the community who wished to remain in the community had to comply with the rules. Even married men were forced to have filtered Internet, with the power to whitelist individual websites delegated to their wives, who were considered “above corruption.”

When I was a teenager, I decided I wanted to go to college. This was rare, as most of my school friends and relatives were either forbidden to attend or uninterested in college. Of course, I was not permitted to attend a “secular” college, and was only permitted to attend a specific religious college which I cannot name here for obvious reasons. This college was away from the physical community I grew up in, but followed most of the same rules, albeit in a slightly laxer fashion. Students were allowed to have laptops and, while the college encouraged filters, it did not enforce filtering the Internet.

The laptop which I owned at the time was given to me by my grandfather, and because of the contract my parents signed with the religious high schools in my hometown, the laptop had a very strict filter called K9 installed. YouTube was blocked. However, being in college and a computer science major, I needed access to YouTube coding tutorials! I asked my parents if they could supply the password to uninstall the filter, and they adamantly refused. How could they go against the school contracts?! My younger siblings would be expelled from high school if they found out the older brother used unfiltered Internet!!

However, being a computer science student had its advantages, and I soon learned about Ubuntu. The Ubuntu website was strangely not blocked by K9, despite most standard ways of bypassing web filters like VPNs being blocked, and so I downloaded an ISO and learned to dual-boot Ubuntu alongside Windows. My parents never found out, and now I had YouTube access!

YouTube access was the most exciting thing to me at the time, and I quickly started finding things out about “the secular world.” There was this thing called *anime*, and it was awesome!! There were videos on cults and atheism, which I would eventually watch. And I could finally watch coding tutorials!

Fast-forward several years, and I have finally escaped the cult’s clutches and the clutches of my parents. I work in tech and am living my best adult life on my own terms, and I have Linux to thank for opening my eyes. I dropped out of that religious college, saved up some money, and am now finishing up a degree at a proper “secular” college!

I am looking forward to continued 2600 meetings!

Reflections on Hacking and Teaching at State Universities

by Diana Kanecki

This New Year's, I was thinking of a Christmas greeting I had gotten from a friend who recently retired as a professor at my alma mater. We are similar, and both of us started the same way - working in the field and then moving into the role of professor. Another friend who is still teaching at our alma mater interviewed for the same professor position as me in 2000. I was offered the position first and, at that time, I felt the greatest use to the future was for me to stay in the private sector. My friend accepted the offer to go into the public sector from the private sector as a professor.

I visit my alma mater about once every two weeks to talk with friends who work within the university, and they talk with me about being semi-retired from the private sector, albeit my additional studies included the University of Phoenix where I earned an MBA and have a Doctor of Management (DM), all but a dissertation. When I compare how computer science and even EECS (electrical engineering and computer science) work towards making and understanding how things work, rather than just Android programming and JSON, I am shocked.

Let me explain. As part of my semi-retirement, I audited classes in theater and communications, which included a program on the college radio station WIPZ called *Ideas with Diana* that I did solo, and later was joined by friends Ron and Nikita. The three of us would bounce off each other - and to the students were considered the unofficial "real" professors they wished they had in their classes. As part of the opening, Ron would read from the *Chicago Tribune* about this day in history, I would read and summarize articles from local papers like the *Tribune*, *Milwaukee Journal Sentinel*, *Kenosha News*, *Racine Journal Times*, and the student newspaper *The Ranger News*, discussing things like financial planning for living off campus. Nikita would add humorous comic relief.

Also, the three of us would talk about our careers and our service. Ron is a former noncommissioned officer in the Navy (serving during Vietnam) and prefers to hear "I respect your service" rather than "I thank you for your service," as Ron feels it to be true and not PC. With me, it was the first Gulf War of Desert Shield / Desert Storm, medical support, and solving problems for the Navy and Air Force as a civilian who worked closely within the current environment. Nikita is an artist who studied in

New York at Parsons and received her degree from there, having an art career and being a businesswoman working for a major health supplement company.

So, on our show we would discuss events that the students needed to know, along with occasionally playing music. One time, I heard a remake of "I Will Survive" made in 2018. Afterwards, I modified the playlist and put on the *original* Gloria Gaynor "I Will Survive" and it was fun to see everyone get up and dance.

In addition, we would talk with the students about the dangers of certain types of employment contracts and schemes such as sweetheart contracts, and the hazards of being hired at will and at term, along with the consequences of each. Most importantly, we would encourage students that *it is OK to question your professors*. The reason we had to state this is because even from 2016 to 2020 when our show was on the air, the 60s attitude and awareness was being washed away. Ron had gone to college in the 60s, Nikita in the late 70s, and I had gone to college at age 14 in the 70s and matriculated in the 80s. When we went, we were encouraged to chat with our professors and ask questions, along with the idea that everyone was *human* and no one was a *god*, even if they were a "scholar," as they say.

Also at my alma mater, all of our professors encouraged us to address them by their first name. So, my professors were Alan, Norbert, Gene, Beecham, David, George, Alma, and Anna Marie, instead of today when I talk with students who address their professors as "Dr. Dean" and such. All of my professors had advanced doctorates as well and were leading researchers in their day, but they thought it was pretentious to have someone be forced to say "Dr. Dean."

WIPZ was a victim of COVID, and we were a victim of the PC culture, not by students but by others feeling the students needed a filter and monitor - in essence, treating the students as children. The students appreciated that we talked to them as one would talk to another adult - and in a professional manner. Some of the students would rearrange their class schedule to listen to our show and really liked that we said what they were afraid to say - almost like a college/state university Howard Stern.

But we were given the waving finger like The Doors were on the old *Ed Sullivan Show* when the word "higher" was used in the song. With

us, the word was “blackhole” when discussing a current event during the last administration. Our show was suspended for one month prior to being subjected to private talks after the show with the student station director being the one designated to pass the word from the power tower. Also, a few times there was a phone flashing from the power tower chiding us to drop our discussion about preparing to live off campus and whatever we were reading in the established newspapers mentioned above.

So our experiment of teaching within the resources of the university was greatly liked by the students and most of the professors, but they seemed hesitant to admit when they felt they could not talk tête-à-tête.

Turning to education, I went to talk with a friend who had originally started as a professor back when my alma mater had an EECS department (then known as ASCS (applied science and computer science)) and asked what was being done with XBasic on Android and open source, and nudged that maybe it was time to re-teach the way we were taught, rather than just teaching Android and JSON. My friend liked what I said, yet his reaction was as if I was a heretic who had come from the nether world. He even cringed about teaching BASIC again.

I wondered why that was his reaction and I asked him. He, like other professors I talked to, first looked around to see if we were talking one on one without others present and shared that the administration of the business, economics, and computers department did not want to make waves. It was always like living the song “Der Kommissar” from the 80s when Berlin had two zones during the Cold War.

So my solution was something I learned a long time ago: innovative ideas start with hacking and with the private sector. This is where I asked Ron and Nikita to help add this to our radio and provided course material via social media.

In another example, as part of continuing education, I had a graduate computer science course at my alma mater on computer security. The course was taught by a friend who had recently retired. During the course, there were days that I could not attend due to my health issues, and sometimes for travel reasons as I did not have a car then; public transportation in the Midwest in mid-size cities is unreliable and very limited. However, on the days I did not attend, the professor noticed that the students did not seem to try as hard and lacked motivation. At one point, my friend called me and asked if there was a way I could come more often and that she could arrange for a ride back along with

a lecture break sooner so that I could take care of my diabetic needs.

The main point my friend noticed was that when studying at the University of Phoenix, part of the studies included leadership which was missing in my alma mater. Students are made to feel like they are just sitting in lectures and admiring the *glory* of their professors, forgoing their learning and development.

My friend asked me if, rather than being part of the course as a student, I would expand my role to act as a visiting professional to work with a group of students in the class. The students were knowledgeable in their skill, yet they were not been challenged to develop their leadership compared to some of the guys in the class. I accepted.

In a last example, while having theater as part of my continuing education, I noticed that there were two computer science curriculums, one based upon Android and JSON (which I feel is very limiting) and the other based upon theater. The computer science program in the theater wing reminded me of computer science and applied science. The students learned how to write code in many languages, build their own theater computer systems, and even integrate with hardware for theater effects. Wow!

When I observed this, I thought if I had children, I would recommend that they study computer science in the theater wing. I feel sorry for saying this, as many friends teach computer science in business.

My point from the various examples is that campuses are losing what many of us learned from the 60s through 80s that allowed us to grow beyond our studies, start businesses, begin publishing companies, and move society forward.

In the last year, I have become a maker playing with Arduinos and experimenting with old digital computer interfacing and development. In one project, we made an 8-bit CPU using TI 74LS181 arithmetic logic units (ALUs) - two 4-bit ALUs linked to 64K ram with four registers. We worked in biomedical engineering, where we built biomedical equipment from scratch for uses such as heart monitoring and sound/music. We’ve designed projects that work with ICs, transistors, and biomedical engineering to port the Arduino and ESP units. For me, it is an awakening and a welcome; yet, at my alma mater today, the methods I describe here are thought of as ancient ways that have disappeared into the nether. But they shouldn’t disappear, as makers, as hackers, as tinkerers - tyro culture is always needed to move society forward.

INTERUPTION

by Alexander Urbelis

To My Mother

alex@urbel.is

On July 31, my mother passed away. It was her birthday. And it has been difficult to think deeply about anything but that event. So, with this column, which I dedicate to my mother, I offer my thoughts on her life, her sacrifices, and the uniqueness of raising a hacker in the 1990s.

If you've been reading this column or listening to *Off The Hook*, you will no doubt have some understanding of my fondness for poetry. One of the most meaningful poems I've read is "The Heart Asks Pleasure First" by Emily Dickinson. At only eight lines of text, that poem is a true transistorization of life itself: with brevity and clarity, the poem describes five distinct stages of life. I've taken each of the stages of Dickinson's poem and added my own words, using them as the framework for expressing my mother's impact on me during that stage of her life and my gratitude for all that she gave.

On account of the power and mystery of words, there are several valid interpretations of this Dickinson poem, but I prefer the theory that each line is an encapsulation of a distinct stage of life as the interpretation with the most power and profundity.

Unpacking those stages looks like this:

The heart asks pleasure - first - Birth and infancy; the pleasure principle applies; the stage of life during which one's personality is beginning to form.

And then - excuse from pain - Adolescence; that time in life when you only want to do things that are fun and getting oneself into trouble seems all too easy.

And then - those little anodynes that deaden suffering - Adulthood; when life has a routine that can grind you down and we look for escapes from diurnal regularities.

And then - to go to sleep - Old age; when most of our work is behind us and we yearn for rest.

And then - if it should be the will of its Inquisitor, the liberty to die - Death; when the machinery of bodies begins to fail and health is flagging; that time that will befall us all when death appears as not something to be avoided, but welcomed.

I have also tried to keep true to Dickinson's overall scansion. Each stanza contains lines of only six syllables, ending with a line consisting of eight syllables. Because of this, it was difficult to express

specific memories or concepts and required me to think more abstractly and generally. Astute readers will also notice the last stanza contains a reference to another column of mine (i.e., 41:1).

It is my hope that some or all of these thoughts and feelings will resonate with readers. Anyone who has raised a hacker, our mothers especially, has had to put up with a great deal of nonsense, trouble, and heartache. But there is also mirth; hopefully laughter was as big a part of your upbringing as it was in mine. As the torch of our parents' generation begins to dim, here's to the men and women who made us what we are, and to keeping true to our obligation of passing on that spirit of rebelliousness.



The heart asks pleasure - first -

You knew me from within,
Ensconced by your laughter:
A herald of my youth,
You planted the seed of dissent.

And then - excuse from pain -
Knowledge, mischief, the same,
Telephone lines engaged,
Call waiting enraged us;
You alone kept my conscience
true.

*And then - those little anodynes
that deaden suffering -*

Your daily work, our bread,
My mouth fed, my wings spread:

You alone sent me forth
With your love, to play, to
question.

And then - to go to sleep -
To teach, to laugh, to smile,
These promises we keep;
Your candle burns within;
Tempus fugit, corpus tardat.

*And then - if it should be
The will of its Inquisitor,
The liberty to die -*

Proud of your might and fight,
Never once sad, now free;
Your defiance is me,
Watched over by your loving
grace.



*Written for my mother,
Diane Mcentee,
July 31, 1952 - July 31, 2024*

Journey of a Hacker: From Curiosity to Advocacy in Fairfax County

by Dr. Harry Jackson

My journey as a hacker in Fairfax County, Virginia, diverges significantly from this stereotype. It's a story of exploration, revelation, and advocacy, driven by a desire to understand and improve the systems that govern our daily lives. My own initiation into this world was driven not by malice but by a profound curiosity, an insatiable urge to delve into the intricate matrix of systems that underpin our technological and societal fabric. This article explores the genesis of a hacker's mindset: a narrative far removed from the stereotypical hacker, and rooted deeply in a quest for understanding and exploration.

Curiosity: The Heart of Hacking

At the very core of a hacker's ethos lies curiosity. For me, this was a deep-seated yearning to unravel the complex inter-workings of systems. This curiosity extended beyond the binary realm of code and algorithms, reaching into the ways these digital constructs interact with human-designed policies and the people who are governed by them. It was a fascination not just with how things work, but why they work the way they do, and how they could potentially work differently.

This exploratory drive is akin to that of a child dismantling a toy to see what's inside, not to break it, but to understand it and perhaps to reassemble it in a way that it performs a function never initially imagined by its creators. The hacker's journey, therefore, is one of constant learning, questioning, and reimagining.

The Enterprise Architect Approach

My approach to hacking mirrors the methodologies of an enterprise architect. This involves a holistic understanding of systems - not just in isolation but as part of a larger, interconnected network. It's about comprehending the full spectrum of a system's capabilities, limitations, and its place within a broader ecosystem.

In this context, hacking becomes an exercise in systems thinking. It's about understanding the architecture of a system in its entirety - from the base code that drives it, through to the user interface and beyond into the realm of its real-world implications and interactions. This comprehensive understanding is crucial, as it allows a hacker to see beyond the intended use

of a system, identifying ways it can be adapted, improved, or, in some cases, exploited.

Uncovering Possibilities and Vulnerabilities

Contrary to popular belief, the hacker's mindset is not inherently about causing harm. Instead, it's about uncovering possibilities. By understanding a system deeply, a hacker can identify new ways it can be used, pushing the boundaries of its original design. This might involve repurposing existing features for new, innovative applications or combining systems in ways their creators never envisioned.

However, this deep understanding also brings with it the ability to recognize vulnerabilities. Identifying these weaknesses is not about exploiting them for personal gain; rather, it's about understanding the potential risks and, where appropriate, working to mitigate them. This aspect of hacking is crucial in a world where technology is increasingly pervasive and integral to our daily lives. By identifying and addressing these vulnerabilities, hackers can play a pivotal role in safeguarding systems and protecting users.

Ethical Considerations

An ethical hacker uses their skills to improve systems, whether by enhancing their functionality, making them more secure, or using their insights to advocate for changes in policy or practice. This ethical approach is fundamental to the hacker's ethos, underpinning every exploration and investigation they undertake.

The genesis of a hacker's mindset is a tale of curiosity, exploration, and ethical responsibility. It's a journey that goes far beyond the cliché of the lone hacker in a dark room, penetrating systems for nefarious purposes. Instead, it's a path characterized by a relentless quest for knowledge, a deep understanding of complex systems, and a commitment to using this understanding for positive change.

In a world increasingly dominated by technology, the role of the ethical hacker is more important than ever. By understanding systems, uncovering their potential and vulnerabilities, and adhering to a strong ethical code, hackers can play a crucial role in shaping the technological landscape for the betterment of society. This is the true essence of a hacker's

mindset - a blend of curiosity, knowledge, creativity, and a steadfast commitment to the greater good.

Living in Fairfax County: A Unique Vantage Point

Fairfax County provided a unique backdrop for my hacking endeavors. As a wealthy and technologically advanced region, it's home to a top-rated school district and a population that values education and innovation. However, beneath this veneer of prosperity, I observed systemic issues that needed addressing.

The pandemic unveiled the fragility and shortcomings of our systems, especially in the education sector. Parents, myself included, got an unprecedented view into our children's education, revealing not just academic challenges but also issues with data privacy and administrative accountability.

The Role of a Hacker in Educational Advocacy

As a custodial parent, my journey took an unexpected turn into the world of educational advocacy. I applied my hacker mindset to understand the local school systems - their policies, practices, and their impact on students. This wasn't just about gaining an advantage in a custody battle, but about ensuring that my child received the best possible education.

My investigations revealed a disturbing trend of data mishandling and a lack of transparency within the school district. This realization prompted me to delve deeper, using my skills and knowledge to advocate for change.

Professional Background: A Foundation for Advocacy

My background as a naval intelligence professional, acquisition specialist, and information technology specialist provided a solid foundation for my hacking and advocacy work. I understood how to navigate complex systems and how to use policy to effect change.

This expertise was crucial in uncovering the data privacy issues in our school district. When I learned about the unauthorized transfer of student data to Panorama Education and other third parties, I knew I had to act. This wasn't just a breach of trust; it was a violation of privacy that could have long-lasting effects on our children's lives.

Uncovering Data Mining and Security Flaws

In a digital era where data is as valuable as currency, the sanctity of personal information has become paramount. My investigation into

the local school district's practices unearthed unsettling trends of data mining and glaring security flaws, casting a spotlight on the often-overlooked vulnerabilities within our educational systems. This article delves into these discoveries, examining the ethical implications and the dire need for robust security measures to protect our future generations.

The Disturbing Trend of Data Mining

The initial foray into the school district's digital practices revealed an alarming pattern of data mining. This phenomenon was particularly pronounced among low-income students who largely depended on school-issued devices for their educational needs. These devices, ostensibly provided to bridge the digital divide, became unwitting tools for comprehensive data collection.

This practice transcended the boundaries of ethical use of technology in education. It represented a blatant invasion of privacy, where students' data was harvested to construct detailed personal profiles. The implications of this are profound and disturbing: from tracking students' online behaviors to potentially predicting and influencing their future choices. The lack of transparency in the use of this data only compounded the ethical quandaries, leaving unanswered questions about the extent and purpose of this data collection.

Ransomware Attack:

A Symptom of Broader Issues

The district's vulnerabilities were starkly exposed when it fell victim to a ransomware attack. This cyber assault was not just a one-off incident, but a symptom of deeper, systemic security inadequacies. It served as a wake-up call, prompting a more thorough investigation into the district's IT infrastructure.

Through Freedom of Information Act (FOIA) requests, a startling picture emerged. The school district lacked adherence to industry-standard security practices, a fundamental flaw in any institution tasked with safeguarding sensitive information. This deficiency was evident in the absence of robust data encryption protocols and a comprehensive data management strategy. Such oversights not only made the district susceptible to external threats, but also exposed students and staff to potential data misuse and identity theft.

The Consequences of Inadequate IT Security

The ramifications of these security lapses

are multifaceted. First and foremost is the risk to the privacy and safety of the students. In an age where cyberbullying and online predation are rampant, the leak or misuse of student data could have devastating consequences. Additionally, the lack of encryption and data management policies could lead to a loss of trust in the educational system, as parents and students grapple with the fear of personal information being exposed or misused.

Moreover, these security flaws could have far-reaching educational implications. If students and parents lose faith in the safety of school-provided devices and resources, it could widen the digital divide, with students from vulnerable communities being the most affected. This setback could negate any advancements made in integrating technology into education, especially for those who need it most.

The Ethical Imperatives and the Call for Action

The findings from this investigation underscore the ethical imperative for educational institutions to prioritize the privacy and security of student data. This responsibility is not merely a technical issue but a fundamental educational policy matter that demands immediate and decisive action.

The call to action is clear: educational institutions must adopt and rigorously implement industry-standard IT security practices. This includes establishing robust encryption protocols, developing comprehensive data management policies, and conducting regular audits and updates of their security infrastructure. Furthermore, there must be transparency in how student data is collected, used, and protected, ensuring that the rights and privacy of students are upheld at all times.

The investigation into the school district's data mining practices and security flaws paints a cautionary tale for educational institutions worldwide. In an increasingly digitalized educational landscape, the protection of student data must be paramount. This is not just a technical challenge, but an ethical obligation to safeguard the trust placed in these institutions by students, parents, and society. We need to ensure that technology serves as a tool for empowerment and learning, rather than a threat to privacy and security. The future of education depends on our ability to protect and nurture the trust and safety of our students in the digital world.

The Hacker's Ethos: Advocating for Change

My journey as a hacker in Fairfax County taught me the importance of questioning authority and challenging the status quo. In a world where data is power, protecting that data, especially for the vulnerable, is paramount.

As hackers, we have the skills and knowledge to uncover truths that others might miss. We can see beyond the surface, identify weaknesses, and advocate for better practices. But with this power comes responsibility - the responsibility to use our skills ethically and to effect positive change.

The Message to Aspiring Hackers

At its core, hacking is about a deep understanding of systems - how they work, how they fail, and how they can be improved. This understanding goes beyond mere technical proficiency; it encompasses a holistic view of the system in its entire context, including its interactions with people and policies. As an aspiring hacker, your goal should not be to exploit these systems but to explore them, to push the boundaries of your knowledge and understanding. It's about finding the flaws and vulnerabilities not for personal gain, but to contribute to building stronger, more secure systems for everyone.

Curiosity as a Driving Force

Curiosity is the lifeblood of a hacker. It's the relentless quest for knowledge that drives you to dig deeper, to go beyond the surface level, and to understand the "why" and "how" of things. This unquenchable curiosity is what will lead you to discoveries and innovations that others might miss. It's about looking at a system and asking, "What can this do?" and more importantly, "What *should* this do?" Remember, every great innovation in the field of technology started with a simple question born out of curiosity.

Persistence in the Face of Challenges

The path of a hacker is strewn with challenges and obstacles. You will encounter complex systems that resist understanding, and you may face opposition from those who don't understand your intentions. In these moments, persistence is your greatest ally. The ability to keep going, to keep exploring and learning in the face of adversity, is what separates the truly great hackers from the rest. Remember, the most rewarding breakthroughs often lie just beyond the toughest challenges.

Ethics: The Hacker's Compass

Ethics must be the compass that guides every

aspiring hacker. In a world where your skills can have profound impacts, how you choose to use them defines not only your career but also your character. Use your skills to shine a light on hidden truths, to protect those who are vulnerable, and to advocate for those who cannot advocate for themselves. Be a force for good, a defender of privacy, and a champion of security. When you encounter those in power who seem unaccountable, use your skills to question, to hold them to account, and to bring transparency where there is obscurity.

Advocacy Through Hacking

Your skills give you a unique ability to advocate for change. Whether it's exposing security flaws to prevent cybercrimes, or revealing data misuse to protect individual privacy, you have the power to make a significant impact. Use this power wisely and responsibly. Strive to be a hacker who not only understands systems but also understands the responsibility that comes with this knowledge.

As you embark on your journey as an aspiring hacker, carry with you the principles of understanding, curiosity, persistence, ethics,

and advocacy. Let these be the guiding stars in your exploration of the digital world. Remember, hacking is not just about what you can do with technology; it's about what you *should* do with it for the betterment of society. Your journey is not just a technical one; it is a moral and ethical one as well. Embrace this path with integrity, and you will not only excel as a hacker but also contribute positively to the world.

My journey as a hacker in Fairfax County has been about more than just technology. It's been a journey of discovery, advocacy, and change. Through my experiences, I've learned the importance of transparency, accountability, and ethical behavior, not just in technology but in all aspects of society.

As hackers, our role can be profound. We have the ability to see things others don't, to uncover hidden truths, and to use our knowledge for the betterment of society. My story is a testament to this power and a call to action for other hackers to use their skills for good.

Dr. Harry Jackson is a former Fairfax County Public School Board candidate and parent advocate.



THE HOPE XV FLASH DRIVE

Introducing our latest collection: every talk that was given at this summer's HOPE XV conference on a 256gb flash drive!

Each talk is available as a video or audio file and can be copied to any device of your choosing or shared with as many people as you wish.

This was our latest conference at our new location at St. John's University in Queens, New York City. It was our first un-masked, in-person event since 2018. You can experience or recapture the excitement that was in the air for all three days. A full lineup of talks can be found at xv.hope.net.

Also included is an easy-to-navigate digital guide to all of the talks.

Just **\$89** (plus shipping) for a gigantic reusable drive crammed full of talks from HOPE XV.

Full details at **store.2600.com** or write to 2600, PO Box 752, Middle Island, NY 11953 USA.

Keeping Hacker Culture Alive

by c7five

It was the summer of 1990. I was 15 years old. I spent most of my time navigating Chicago area BBSes like “Temple of Pong” and “Lunatic Fringe.” I’d chat with local hackers, read message board posts on how to make free phone calls or get “unlimited” tokens at the arcade. We’d have regular meetups where I’d need to sneak out of the house after my parents went to bed and hitch a ride to an IHOP. Over pancakes, I’d engage in discussions about government surveillance, the latest warez, and learned more about how being curious shouldn’t be a crime.

People would also bring back issues of *2600* to these meetups. I’d flip through the pages and marvel at how I was holding center of the hacker culture universe in my hands. For a kid who spent most of his time in the digital world, the physical copy of *2600* was magical. I’d save up the money I would get for cutting my neighbor’s lawn and hop on my bike to ride ten miles one way (not an exaggeration, I just mapped it out to be sure) to the nearest Barnes and Noble. It was always a bit of a hunt because the rumor was that the store managers didn’t like hackers and they would always hide copies of *2600* behind the teen or gardening magazines. I probably made this trek eight or ten times in high school. Even as a teenager, learning about hacker culture was important to me because it was helping me discover who I was and wanted to be.

Fast forward 16 years after I graduated high school, I was thinking about the hacker culture in

Chicago and how it was fractured and meetups were inconstant at best. I started to wonder why there wasn’t a true hacker conference in Chicago like H.O.P.E. in New York City and decided I’d start one.

I had zero experience with running on a conference, so much of what I did was learned or through research. In the fall of 2009, I, along with some local hacker friends, announced the first THOTCON would be held in the spring of 2010. The name is taken from the first area code in Chicago, 312, or THree One Two CON.

From the very start, we wanted this event to be a hacker conference, not a security conference. We didn’t want any vendors to influence the topics, the speakers, or ever try and censor a talk while holding a sponsorship check over our heads. We wanted a conference where speaking with handles or highly controversial topics was the norm. We don’t broadcast or record our talks, so there is nothing that can be censored in the future.

Next May 30 and 31 will be THOTCON 0xD. This is our 13th conference which, after COVID, is only held every other year. The first batch of tickets went on sale October

1st (2024) and the remaining will be sold on January 1st (2025).

If we sell all the tickets, there will be nearly 2,000 hackers at an undisclosed Chicago location (greetz FBI). The call for papers will also open on October 1st. Please consider speaking or attending THOTCON 0xD and helping keep hacker culture and conferences alive in the world.

Thanks for reading!



Lee Williams, Harassment Agent Episode 3

by Lee Williams

(This story is a complete work of fiction.)

Washington, DC

Pierre pulled to the side.

“Holy shit,” I said. “That was something.”

He turned and looked at me, like this was my fault, but didn’t say anything.

“What?” I asked.

“So, are they killing me and you when they clean house? Or just you.”

He knew that I knew the answer, but it also wasn’t me who got him into this mess. He was just in it.

“Whoever gave you this number -”

“Leon. Leon *fucking* Manna.”

“Okay,” I said. “Leon either didn’t know about this or wants you disposed of.”

“Motherfucker... I should have gone to Ireland like he said.”

“What the hell even happened?”

“I don’t know,” Pierre said. “I was friends with this junkie lawyer named Lenny... Using

that word, lawyer, loosely... And then he introduced me to this drug-addled hacker type named Leon. They needed me to steal a boat. Anyway those two idiots got arrested in Miami and I dipped before they could nab me too. They managed to beat most of their cases, somehow. And then I got locked up for getting in a bar fight that turned into a murder and called Leon, who told me to call a number, which I did. Next day the warden said I was being released. When I got out, some old bald guy with a mustache picked me up, said I had to pay, and that I was theirs now. So he sent me to that bar you met me at.”

“That was Ray. I assume Leon didn’t screw you then, but they’re still gonna take you out anyway. That’s what they do.”

“Have they ever done this before?” he asked.

“I only saw them do it once... Everyone was wiped out of the organization except for me and Valentina. I think I was 19.”

"How old are you now?"

"21."

"Christ. So what do we do?" Pierre asked.

"We have some options. But I think our best bet to stay out of jail is to stick to murder capitals. Alternatively we can go out of the country. Like a bitch. My aunt has a house in Canada. Well, she did. It's mine now."

Pierre was silent.

Me and Pierre went downtown and got coffee. We sat down at a coffee shop in some rich, stinking neighborhood called Georgetown. Named after a dead president who was here all those years ago... And here I am now. Again.

Then me and him walked to an Irish pub near the waterfront.

Sitting in the bar, we hatched a plan.

I sipped my Modelo. "We could go to Cuba."

"Nah," Pierre said. "I knew a guy who tried to do that."

"And?"

Pierre laughed. "It was one of the guys I was talking about. Leon. Lenny the Lawyer's friend. He got arrested on the dock. And then by the grace of god, somehow, didn't get incarcerated for any of the stuff he did. He got lucky, a bad prosecutor and a lazy judge. He pled guilty to some drug charges though."

"Well," I asked. "Where are they at now?"

"Lenny Cruz, his friend, is dead. Leon is alive, kinda."

"What do you mean?"

"Eh... his brain is kinda... done. Or some part of him is not the same. It's hard to explain. He's on drugs, I think."

"You have a warrant for your arrest, right?"

"What does it matter," he said. "We're fucked one way or another."

I had a flashback to being a teenager, here, in DC. I remembered one of the guys who saw me grow up. I knew he was still here. But some deep, instinctual part of me knew that it wasn't the time to reach out.

Arlington, Virginia

I mixed some of my crypto, sold it at an exchange, withdrew it to my bank account I have set up under someone else's name, and went out to a shitbox motel in Arlington, Virginia to get a bus ticket somewhere else. That could all change if That Friend Of Mine picks up.

"It's 50 degrees right now," I said to Pierre. "It's going to be 25 degrees there and it's snowing. My aunt's house has no heat, and we'll need snow tires. She lives off a dirt road."

"So what the hell do we do?"

"I say we go south. I wanna go to South Carolina. Or Florida."

"Whatever dude, at this point I've kind of accepted my fate," he said. "Just don't get us arrested."

"Arrested? I was planning to just pump fake on the cops. Hopefully they'll shoot me."

I canceled the tickets and bought another set for Jacksonville, Florida. The next available bus was at two in the morning, but I decided to take it anyway. We arrived at the bus terminal and got on. I took some Seroquel, and passed out.

I had a dream on that bus ride.

It was when I got pinched in 2022. Last time I got grabbed. For possession of marijuana. And then somehow JB was involved, and I remembered his email, which he never, ever got locked out of no matter what. And I reached out and the whole time he wasn't dead.

And then I was driving down Atlantic Boulevard, in Morehead City, North Carolina, and a girl was in my passenger seat. Can't remember who, but it was someone from a long time ago. Someone who I thought I had forgotten. And I was just driving down the road, citation flying out the window, but I was still gonna go to my court date. If I didn't, they'd put a warrant for my arrest. And then I crashed out into a pole.

I was standing at a payphone, under a palm tree in some downtown area. Bell South, or Bell Atlantic, or something. It was night time. I started smoking Lucky Strikes. The street lamp was flickering. Suddenly that phone rang.

I picked it up.

"August," a female voice said. "They're gonna get you."

I could recognize that voice anywhere. It wasn't Valentina's. It was a girl from another life that I lost a long time ago.

"I think," I said, heavily, "you have the wrong number."

"No. You don't really look like a Lee, you know that? Always thought you looked more like an Anthony. You may as well have stuck with an Italian name."

"Whatever."

"This dream you're living in is silly," the familiar voice said. "Don't go to Jacksonville. Bad things are waiting for you there. What are you doing?"

"I'm going," I said. "I'm sorry."

Suddenly I wasn't on the phone anymore, I was on a couch, in the abandoned house, in Maryland. I was 19. Andres was standing by the window. Looking out at flashing lights. Then turned to look at me.

I woke up in South Carolina, took a piss, and dreamed a dreamless sleep until I woke up

in Jacksonville. I wrote an email to JB, with absolutely no idea if he'd even receive it, and booked a motel on Airport Road. Pierre was nowhere to be found, but he had my Signal. I checked in via a cab and fell asleep in the motel. At 5 AM I awoke to my Signal ringing.

INCOMING CALL: UNKNOWN

I picked it up.

"Hello?" I said sleepily.

"Is this August?"

I snapped up in bed immediately. I know that accent. "John?"

"Yeah."

"Jesus Christ, I thought you were dead. Yeah, it's me. I go by Lee now."

"No, I was committed to a mental hospital. And you don't look like a Lee."

"Welcome back, I guess," I said. "How are you doing?"

"By now I've made over a million dollars and am in the top 1% of my country."

"I assume you have some work you need done, then."

"Yeah," he said. "Do you need help?"

"I'm in deep shit, John."

We spent the next couple hours on the phone and messaging via Signal discussing what was going on with him and me, until the sun rose. I told him I was in Jacksonville, and he asked why.

"I'm running."

He was quiet for a second, over the phone.

"Since we fell out of contact," he said. "I got rich. And I think, after all the favors you've done me, as a foot soldier... the no pay jobs you did... and sticking through all the shit I had going on... I'm giving you and someone else 10k."

"What do you mean," I said. "Someone else?"

"I've had multiple constituents this whole time."

"Yeah," I said. "I figured that much. I had a feeling it wasn't just me."

"You're each getting 10k, for helping as my main constituents."

"God bless you," I said. "I really did think you were 6 feet."

"No. I needed the meds, though. I was manic."

By 8 AM, Pierre was nowhere to be found and I was alone in Florida. I looked around, and tried to make something of my situation. HHH, it is evident they don't want me anymore. Johnny is back though, Johnny Boy. And this third figure who I have yet to speak with. And now I had an extra 10k in my pocket.

The first part was getting more. It was apparent to me that Bitcoin was on an up-and-up type wave, so I made sure to keep it in BTC so I could keep earning every day. And when it seems like the price has gone so far up, and you've won so much you feel tired of winning, that's when you pull.

I also needed a place to discreetly rent. If you ever want to discreetly rent, go on Craigslist. I looked around for a while, until I found a place, and reached out. It was a short drive out of Jacksonville, way out in the swamp, called Baldwin. I checked out the room, and everything looked good. Then I used the money from that aforementioned up-and-up to put down a deposit. Finally, when they asked for ID, I showed them the one that says "Lee Williams."

In case it wasn't apparent, I've been living under a number of synthetic identities for 2 years. I do this with a combination of realistic false documents, credit privacy numbers, and lies I tell myself and the people around me. Credit privacy numbers, in particular, I find interesting. There's a website that anyone can access where you can check whether an SSN is in use or not. If you find one that *isn't* in use, you can then work with that to slowly and surely create a "fake person" if you put the right info in the right places. And with that, you can open lines of credit, rent cars, the whole 9 yards. But me, I was never flashy with it.

And all this took, to rent a living space, was just a picture of my false documents.

I looked out at the sunset from my window. I was tired. I didn't want to think. My mind couldn't take it anymore. The place and time I was at the beginning of this story had already started to feel foreign to me. I wasn't sure how much more I could endure. I didn't know where Pierre was, or if I could even call any of my old associates, or if I should do anything at all. And my standing with Johnny Boy, it's back. Where I go from here is completely unknown to me. But at the very least, it's a known unknown. I'm aware of its existence, or lack thereof. But would they find me here?

What if I went in circles? What if I traveled constantly, never staying in one place too long? What if I ran and made them run?

And as for if I'd ever get my get-back on Ray, I'll find out.

7 missed calls from Valentina Garcia.

Soundtrack

Track Meet - Migo Lee

Cold Blood - Peter Tosh

It Was Only A Dream - Joey Quinones

Duke Of Earl - Alton Ellis

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally don't cost a fortune and are open to everyone. If you know of a conference or event that should be known to the hacker community, *email us* at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA**.

Please remember that we need sufficient lead time (a minimum of three months) to list events in the magazine. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community. All events are subject to change.

October 25-26

SecureWV 15

Charleston Coliseum
and Convention Center
Charleston, West Virginia
www.securewv.org

October 25-27

Maker Faire Rome

Gazometro Ostiense
Rome, Italy
makerfairerome.eu

November 9-10

Maker Faire Orlando

Central Florida Fairgrounds
and Expo Halls
Orlando, Florida
www.makerfaireorlando.com

December 27-30

Chaos Communication Congress

Congress Center Hamburg
Hamburg, Germany
www.ccc.de

February 15-16, 2025

Vintage Computer Festival SoCal

Hotel Fera Anaheim
Orange, California
vcfsocal.com

April 4-6

Vintage Computer Festival East

Infoage Science and History Museums
Wall, New Jersey
vcfed.org

May 16-18

CackalackyCon

DoubleTree at Research Triangle Park
Durham, North Carolina
cackalackycon.org

May 30-31

THOTCON 0xD

Chicago, Illinois
www.thotcon.org

August 7-10

DEF CON 33

Las Vegas Convention Center
Las Vegas, Nevada
www.defcon.org

September 6-7

Blue Team Con 2025

Fairmont Chicago
Chicago, Illinois
blueteamcon.com

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

AZ 00000000 A
A1

UNITED STATES
OF AMERICA



Marketplace

AZ 00000000 A

20

For Sale

THE RADIO PHONICS LABORATORY: *Telecommunications, Speech Synthesis, and the Birth of Electronic Music* by Justin Patrick Moore, KE8COY. Set your receivers for a mesmerizing story found at the intricate intersection of technology and creativity, spanning a century of discovery from the 1880s to the 1980s. Explore the path of this circuit diagram that connects telegraphy and the invention of the telephone with radio laboratories and the advent of our global communications systems. At the heart of this narrative is the evolution of speech synthesis and the quest to make a machine capable of speech. This groundbreaking innovation not only revolutionized telecommunications but gave birth to a new era of electronic music. Tracing the origins of synthetic speech at places like Bell Laboratories and its applications in various fields, *The Radio Phonics Laboratory* unveils the pivotal role it played in shaping the creative vision of sound pioneers, maverick musicians, and experimental luminaries. This is the story of how electronic music came to be, told through the lens of telecommunications scientists and electrical engineers. This is the story of how electronic music started with the dits and dahs of Morse code and transformed into the blips and bleeps that have captured the imagination of musicians and dedicated listeners around the world. Published by Velocity Press and available in the UK and Europe from velocitypress.uk. In North America find *The Radio Phonics Laboratory* on Bookshop.org, that one big company named after a jungle, and fine bookstores everywhere.

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From RF Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers, red teamers, and penetration testers need. Check us out at <https://HackerWarehouse.com>

BUTTERFLY is an innovative and patented indoor air quality (IAQ) monitoring system including a suite of beautifully designed hardware with glowing wings, integrated software, and a charming narrative that has been developed at Imperial College London over the past 4 years. Our highly qualified UK team has engineered a new standard of accuracy and reliability which meets and exceeds the international WELL standard for buildings. Butterfly IAQ data is consistent and trustworthy, providing for integration with air purification technologies to deliver >40% energy savings in buildings - an industry first. Our products are manufactured in the UK from recycled materials to matchless standards of quality to ensure long term durability and service. 1% of our profits will be donated to the Butterfly Conservation Organization. Until now we have lacked the tools to measure and react to contaminants indoors. Butterfly solves this challenge in a sustainable, trustworthy, and responsible way. We have a carefully considered suite of products which can be flexibly installed in a hub & spoke arrangement to suit a wide variety of buildings: Our secure IOT platform enables clients to monitor and manage the safety, efficiency, and trend of air quality. Check us out at butterfly-air.com

SECPOINT PENETRATOR SOFTWARE: WiFi Pen Testing (WPA WPA2 WPS). Vulnerability Scanning & Assessment. Multi-User Support for MSPs. Customizable Whitelabel Reports: Add logos, names, watermarks. Reports available in PDF, HTML, and 19 languages. Get 26% off Coupon Code: 2600 <https://shop.secpoint.com>

HACKS, LEAKS, AND REVELATIONS: *The Art of Analyzing Hacked and Leaked Data*, by Micah Lee: The world is awash with hacked and leaked datasets from governments, corporations, and extremist groups. This data is freely available online and waiting for anyone with an Internet connection, a laptop, and enough curiosity to analyze it. Want to use your hacker skillz to change the world? Check out my new book at hacksandleaks.com. You'll work with real datasets like hacked police docs, chatlogs from a Russian ransomware gang, videos that Jan 6 insurrectionists uploaded with GPS coordinates, and a lot more.

HACKERBOXES is your monthly subscription box for hardware hacking, DIY electronics, cybersecurity, and hacker culture. Each monthly HackerBox includes a carefully curated collection of projects, components, modules, tools, supplies, and exclusive items. A HackerBox subscription is like having a hacker convention in your mailbox every month. Free online educational material, free domestic shipping, cancel anytime. Visit us at www.HackerBoxes.com for workshops, boxes, merch, and more.

COOL SOLDERING KITS FOR SALE! TV-B-Gone for turning off TVs in public places. ArduTouch music synthesizer kit for making beautiful music, sound, and noise. And more! Learn and grow and do cool things. Everyone can solder! Step-by-step instructions show you how. All ages, friendly for total beginners. <https://CornfieldElectronics.com>

PHONECO INC. has old oak crank wall phones, desk phones from 1892 to the 1980s, parts, old 3-slot payphones, walnut and oak ringer boxes, Ericophones, telephone magazines, telegraphs, switchboards, novelties, decorators, and more. Some display and others stacked up in barns and old semi trailers in the process of elimination. 1905-1972 3-slot payphones \$280, 1892 Eiffel towers \$1200, 1976 copies of the 1892 by Ericsson \$285. A gadget is available (\$79) to permit using

any landline phone on a cell phone line (circuit) - this unit installs right into each old telephone, turning any old phone into a cell phone. Amongst many books are 2200 page "Telephone History" thumb drive or DVD \$38.00 ppd and a 440 page "Payphone History" \$18.00 paperback. Both are heavily illustrated. We consist of two handymen, a buffer, clerical/shipping helper, and Ron and Mary (owners). When all is gone, no replenishment; unable to predict the outflow of inventory. Conversation about old telephones offered freely and charitably. The Phoneco building opens around 2 pm Central Time. Guests are welcome by arrangement or can freely walk in after 2 pm until 8 or 9 pm. Fly into Minneapolis, drive the 130 miles to Galesville, Wisconsin. Two close motels and diners. Accommodations are comparatively inexpensive. Dress warm as most of the buildings are not heated. You can roam freely. And if you have specific interests, we can point you in a direction. We are trying to move out of the large building and sell the business. 608 582 4124 10 am to 8 pm CT. phonecoinc@aol.com www.phonecoinc.com Phoneco, W21975 Hess Rd., Galesville, WI 54630. We will ship worldwide.

Announcements

THE HACKER MINDSET offers a fresh perspective on using your hacking skills beyond the digital world. Garrett Gee reveals how to apply these talents to life's broader challenges. Discover how to hack your way to success in every aspect of your life. Now in print and available at your local book store and major book retailers. Read more at <https://hackermindsetbook.com/2600>

JOIN THE HACKER WIKI! Share your knowledge and learn from others. Contribute tutorials on computing, Linux, and hacking. Help build the ultimate resource for hackers, by hackers. Collaborate, innovate, and elevate the community. Visit <https://hack-the-planet.cc> to start contributing today!

STRAY POINTERS is an interview podcast focusing on people who are doing or experiencing amazing things in a variety of subject areas in tech and the arts. Please look for it on your favorite podcast site or stop by straypointers.com for a complete list of episodes.

THE WORLD OF DATA CENTRES (DCs) have been captured as part of my visual art practice for over 20 years: a visual experience that evolved a visual art form. DCs are machines that process and store data. Demand for data is rising and the development of ChatBot and similar applications boosting requirements. This new technology has evolved from AI and machine learning, operating on an infrastructure network and storage system, supported by power and cooling with critical failure redundancy. The environment within the data centre is an AI platform liberated from human intervention, shaped by technological rationale. A space reflecting a post-human institution requiring human and non-human collaboration. My art examines the DC environment of architecture, industrial and technological photography currently used by DC development owners who have a vision for the value of their DC portfolio and particular brand. My art expresses itself as a creative contemporary addition, exhibited extensively in magazines and exhibitions. These images represent key aspects of the DC machine, using an architectural aesthetic treatment, captured in the perpendicular. I created this art to beautify the soulless, machine environment, and to paint a Kubrick-type vision, whilst asking: is this architecture art, or is this art architecture? jamesreidphotography.com

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the 2600 site in mp3 format! Your feedback on the program is always welcome at oth@2600.com. New for the pandemic: *Off The Hook Overtime*, Wednesdays at 8:00 pm ET on youtube.com/channel2600. Call in at +1 802 321 HACK!

THE THREAT ACTOR'S DIARY is an edgy cybersecurity blog and hacker resource site that's by hackers, for hackers with a podcast on the way. We're also the official Dallas Million Mask March info hub. Swing by and subscribe! Created by GhostExodus, founder of the Electronik Tribulation Army. We accept interviews & article submissions! <https://www.GhostExodus.org> contact@ghostexodus.org <Ghost.exodus.freelance@gmail.com>

HACKER CULTURE: A TO Z by Kim Crawley is now available through O'Reilly Media. It's a fun mini-encyclopedia covering over 300 topics - from notable hackers to tech companies, from hacker ideals to popular technologies. The book is also full of pop culture references and nerd humor. The book contains original quotes from Emmanuel Goldstein and some fun Easter Eggs. Follow news about the book through linktr.ee/kimcrawley, @crowgirl.bsky.social on Bluesky or @crowgirl@hachyderm.io on Mastodon.

VAGUEBOOKING is a podcast about life lived online, and our new series "The People's History of the Internet" covers the history of the early Internet and the hackers who shaped it. Tune in for conversations with Phil Lapsley, Lucky225, Rob T Firefly, and many more! Found wherever you get your podcasts and at vaguebooking.net

Services

KB6NU's "NO NONSENSE" AMATEUR RADIO LICENSE

STUDY GUIDES make it easy to get your Technician Class license or upgrade to General Class or Extra Class. They clearly and succinctly explain the concepts, while at the same time, give you the answers to all of the questions you may find on the test. The PDF version of the Technician Class study guide is FREE, but there is a small charge for other versions. All of the e-book versions are available from kb6nu.com/study-guides. Print versions are available from Amazon. Email cwgeek@kb6nu.com for more info.

TOP TIER FULL STACK IT CONSULTING for all your needs - competitive pricing! We specialize in providing over 27 years of experience in delivering top tier IT consulting services. Our full stack runs the gamut all the way from software, hardware, network and security engineering, and in a wide range of fields such as marketing, art & design, and research. Services include: IT Infrastructure and Network Design (full system and network architecture design using open-source technologies, white-glove support for implemented solutions), Security Services (comprehensive incident response services, security architecture and consultancy, custom tool development for security operations), Legacy System Support (maintenance and support for legacy systems, including those crucial for business continuity), Software Development (custom software development for specific needs, including physical access control and blockchain), Consulting and Advisory (IT and security consulting with a focus on strategic advice and incident response; business development consulting, particularly in the tech and e-commerce sectors), Specialized Projects (development and support for unique and challenging tech projects, such as those beyond what mainstream solutions like Zillow can offer. 31337 IT Solutions http://31337itsolutions.com/

BUSINESS AND TECHNICAL ADVICE AND SOLUTIONS. Got a tough business problem? Need a creative, impactful solution from somebody who understands the tech? I offer strategies and solutions for everything from business growth to data visualization, with a hacker mindset for tackling challenges. Business, startup, or just looking to make some money with your skills, I can help you out. Let's chat. Visit avc.consulting or email hello@avc.consulting and mention 2600.

AFFORDABLE WEB HOSTING & SERVERS: NodeSpace Hosting offers affordable web hosting, email, domains, SSL certificates, bare metal servers, and virtual private servers at affordable prices. We are specialists in Proxmox VE hosting - from standalone nodes to full scale HCI solutions, you can build a private cloud in our data center. The cloud might be someone else's computer, but at least you get root access on ours! Use promo code 2600413 for 10% off recurring discount any shared or reseller plan, VPS, or in stock bare metal server. We also provide free migrations from other service providers! <https://www.nodespace.com>

DIGITAL FORENSICS EXPERTS FOR CRIMINAL AND CIVIL CASES! Sensei's digital forensic examiners hold prestigious certifications including the CISSP, CCE, CEH, CCO, and EnCE. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, theft of proprietary data, data breaches, interception of electronic communications, rape, murder, wire fraud, espionage, cyber harassment, terrorism, and divorce matters. We can preserve, analyze, and recover data from many sources, including computers, external media, smartphones, and social media. Sensei Enterprises believes in the Constitutional right to a zealous defense and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's principals have written 18 books on IT, cybersecurity, and digital forensics published by the American Bar Association. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

CONFLICT INTERNATIONAL is a global intelligence, investigation, and risk management agency providing investigation and intelligence to clients globally. Our network of professional investigators based in jurisdictions worldwide enables us to conduct international investigations effectively and efficiently. Our headquarters are based in central London with offices throughout the USA, Marbella, and Cyprus and the ability to mobilize a team of investigators at very short notice. Our team has decades of experience working with companies, law firms, and private individuals to provide bespoke investigation and intelligence services including fraud, surveillance, asset tracing, assistance in matrimonial and child custody matters together with international risk management. Put your trust in Conflict International and our diverse range of skills developed from backgrounds in military intelligence, security intelligence services, practiced lawyers, and forensic specialists. This enables us to hand pick the right skill set combination of experts to competently conduct your investigation. We use insight, intelligence, investigation, risk management and strategic solutions to solve problems troubling individuals, companies and organizations of all kinds anywhere around the world. We excel at handling complex and sensitive matters, and work at a local, national, or international level with discretion and the utmost confidentiality. Contact your local office: www.conflictinternational.com info@conflictinternational.com

HAVE YOU SEEN THE 2600 STORE? All kinds of hacker clothing, back issues, and HOPE stuff! We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. It's great for giving out presents with a hacker theme - or gift cards are available for those who'd rather make their own choices. The store is constantly getting bigger and more interesting. Please come pay us a visit! store.2600.com or 2600.store

LOCKPICKING101.COM is open to hackers wanting to learn physical security and the insides and out of locks and lock picking. Register to join one of the oldest Locksport communities online.

ANTIQUÉ COMPUTERS. From Altos to Zorba and everything

in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. <http://www.vintagecomputer.net>

UNLOCK YOUR DIGITAL SOVEREIGNTY WITH ENS! In a world where digital identity theft and data breaches run rampant, take control of your online security with Ethereum Name Service (ENS). We believe that everyone deserves to own their digital identity, and ENS is here to empower you. ENS is open source, decentralized, and multichain, making it the ultimate tool for securing your online presence across various platforms and blockchains. With ENS, you can: Safeguard Your Identity: protect your online persona from unauthorized access and cyber threats; Go Multichain: seamlessly manage your digital identity on Ethereum and other compatible blockchains; Own Your Data: say goodbye to centralized authorities controlling your online information. Join the ranks of hackers and digital pioneers who recognize the importance of digital sovereignty. Take charge of your online security and establish your presence with ENS today! Visit ens.domains to get started and let ENS be your trusted ally in the battle for online privacy and security. Your digital identity is in your hands.

ICONOCLASTIC RESEARCH LIBRARY - Visit us in San Francisco to read 2600 in hardcopy going back many years! Take a bite out of Byte, or study radio science. Stacks at the Prelinger Library offer hundreds of feet of books about the history of computing and related technologies, wired in with dozens of other subjects. Browse vintage *Science and Mechanics* and *Computers and People*, or get lost in the zine archives. You may discover a topic you didn't know existed. We offer tea to visitors and collect no information that visitors do not volunteer in our guest book. Drop-in hours as well as remote browsing environment available at www.prelingerlibrary.org. Half the hosting consortium are amateur radio operators. Not a lending library, though we welcome photography and scanning on site, and all items digitized and hosted by our allies at Internet Archive (www.archive.org) are freely downloadable.

CALL INTO THE PHONE LOSERS OF AMERICA'S telephone network interface and hack into our collection of answering machines from the 80s, 90s, and 2000s. Listen to episodes of Joybubble's "Stories and Stuff," old telephone recordings, adventure choosing games, and more! Dial 505-608-6123 or 845-470-0336.

DO YOU HAVE A LEAK OR A TIP that you want to share with 2600 securely? Now you can! 2600 is using SecureDrop for the submission of sensitive material - while preserving your anonymity. Anonymous tips and documentation are where many important news stories begin. With the SecureDrop system, your identity is kept secret from us, but we are able to communicate with you if you choose. It's simple to use: connect to our special .onion address using the Tor browser (2600.securedrop.tor.onion), attach any documents you want us to see, and hit "Submit Documents"! You can either walk away at that point or check back for a response using a special identification string that only you will see. For all the specifics, visit <https://www.2600.com/securedrop> (you can see this page from any browser). For more details on SecureDrop itself, visit <https://securedrop.org>. (SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.)

Personals

AS IS TRUE WITH ALL PROJECTS, things develop. My research into the use of technology within the prison context has found... things. First, I'm not looking for pen-pals. Though I'm not averse to that, it is not my goal. Second, all letters require a return address on the envelope, but it doesn't matter if it's real. Third, I'm interested in all technologies from timers on toilets to computers to video libraries. Tell me the story of its history, what you've done, what you're trying to do, where you think it should go, or policies advancing or limiting technology and learning technology. Tell me about the culture surrounding the stuff; is there a class, a club, is it volunteer or paid programming? Do you hackers hang out? Does the staff target you? This is a broad investigation for curiosity sake, mainly, but I also want to produce a report for the Wisconsin Dept. of Corrections about various uses of technology and how it could be employed to improve living conditions. I'd also like to write a few articles. My address is: Jason R. Glascock #342498, Racine Correctional Institution, PO Box 189, Phoenix, MD 21131. This is a contract remailer the Wisconsin DoC uses and they require the prison's name and my number. It takes ~20 days to get mail. Technology.

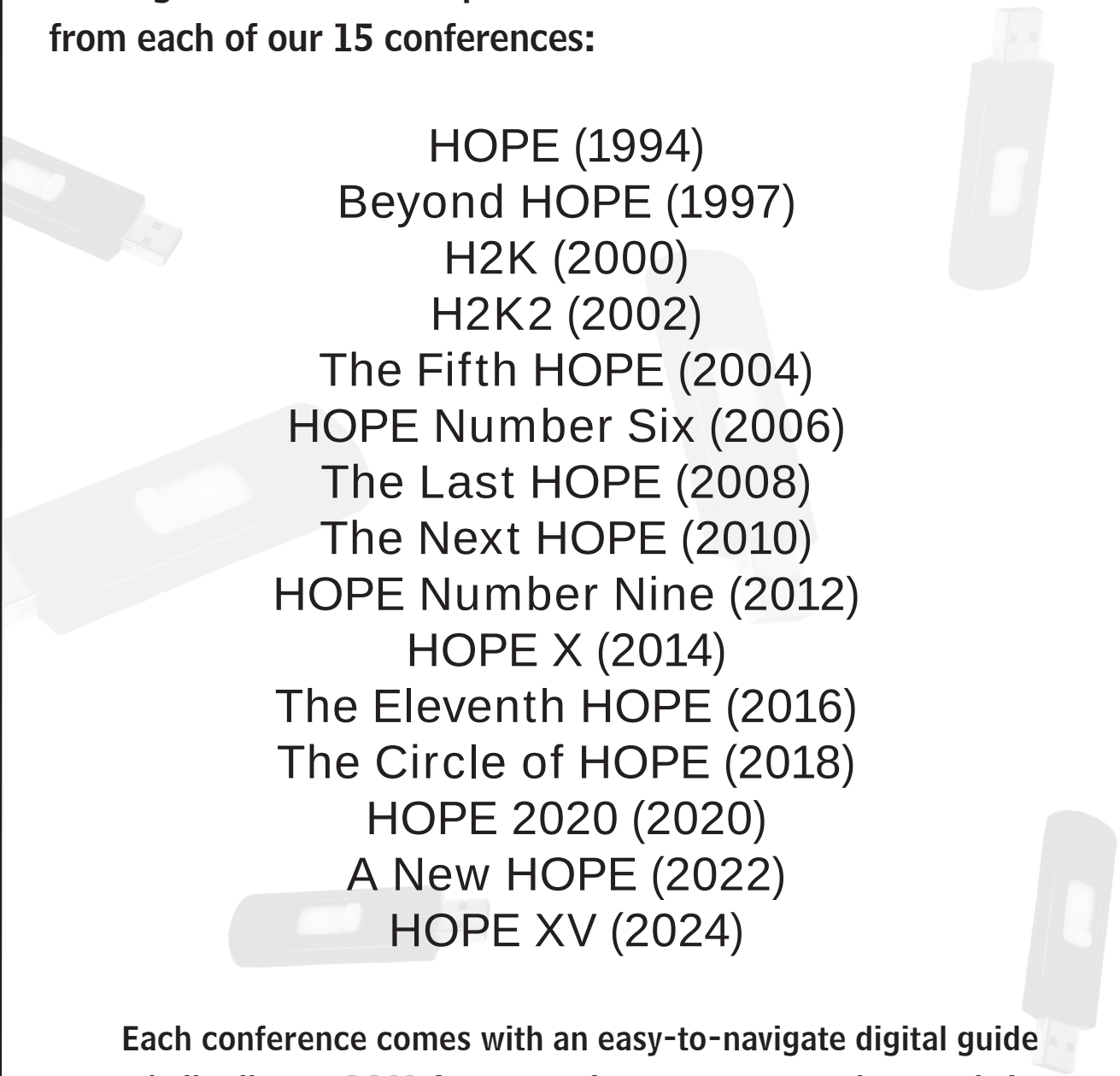
ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. **We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril.** All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include a copy of your address label/envelope or a receipt/customer number so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to marketplace@2600.com.

Deadline for Winter issue: 12/3/24.

ALL 15 HOPE CONFERENCES!

If you truly want to witness the hacker world grow and change, we recommend getting ALL of the videos from each and every one of our conferences. Yes, we saved it all, and we believe it's a must for the library of anyone with an interest in this sort of thing.

You'll get 10 flash drives packed with all of the recorded talks from each of our 15 conferences:



HOPE (1994)
Beyond HOPE (1997)
H2K (2000)
H2K2 (2002)
The Fifth HOPE (2004)
HOPE Number Six (2006)
The Last HOPE (2008)
The Next HOPE (2010)
HOPE Number Nine (2012)
HOPE X (2014)
The Eleventh HOPE (2016)
The Circle of HOPE (2018)
HOPE 2020 (2020)
A New HOPE (2022)
HOPE XV (2024)

Each conference comes with an easy-to-navigate digital guide and all talks are DRM-free, meaning you can copy them and view them anywhere (and reuse all of these drives for other things!).

You can get it all for \$399 plus shipping. Full details at store.2600.com or write to 2600, PO Box 752, Middle Island, NY 11953 USA.

"Peace cannot exist without justice, justice cannot exist without fairness, fairness cannot exist without development, development cannot exist without democracy, democracy cannot exist without respect for the identity and worth of cultures and peoples." - Rigoberta Menchú Tum, Guatemalan human rights activist, 1992

Editor-In-Chief
Emmanuel Goldstein

S

Infrastructure
flyko

Associate Editor
Bob Hardy

T

Network Operations
phiber, olssy

Layout and Design
typ0

A

Broadcast Coordinator
Juintz

Cover
Dabu Ch'wald

F

IRC Admins
honeyp0t, r0d3nt, dclaw

Office Manager
Tampruf

F

Facebook Team
astrutt, Cryovato, TechnoMage,
danixdefcon5, ItsTehPope, JWiley

Inspirational Music: Ministry, Eurythmics, Nasser Halahlih, Barbara Lynn, Stevie Wonder, Petula Clark, Janis Ian, The Electric Prunes, Andy Milonakis, A\$AP Rocky
Shout Outs: Lex Luthor, Delchi, Deth Veggie, DookieX, TS, Wayne Cabot, polybius
RIP: WCBS

2600 is written by members of the global hacker community.
You can be a part of this by sending your submissions to
articles@2600.com or the postal address below.

.....
2600 (ISSN 0749-3851, USPS # 003-176) is
published quarterly by 2600 Enterprises Inc.,
2 Flowerfield, St. James, NY 11780.
Periodical postage rates paid at
St. James, NY and additional mailing offices.

POSTMASTER:

Send address changes to: 2600,
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:

2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:

U.S. & Canada - \$31 individual,
\$60 corporate (U.S. Funds)
Overseas - \$44 individual, \$75 corporate
Digital (PDF and EPUB) - \$19.99 at
store.2600.com

BACK ISSUES:

Individual issues for 1988-2023
are \$7.25 each when available.
Shipping added to overseas orders.
All back issues (1984-2023) available
digitally as annual digests and individually
in PDF format from 2018 on at store.2600.com

LETTERS AND ARTICLE SUBMISSIONS:

2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

Mastodon: @2600@mastodon.online **Bluesky:** @2600.com **Remains of Twitter:** @2600

2600 Office/Fax Line: +1 631 751 2600

Copyright © 2024; 2600 Enterprises Inc.

MEETINGS

**2600 MEETINGS ARE THE BEST WAY TO MEET FELLOW HACKERS!
KEEP CHECKING THE WEBSITE BELOW FOR MORE UPDATED LISTINGS
AS WELL AS INFO ON HOW TO START YOUR OWN MEETING!**

ARGENTINA

Buenos Aires: Bodegón Bellagamba, Armenia 1242. 1st table to the left of the front door.

Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499. 7 pm

AUSTRALIA

Melbourne: Oxford Scholar RMIT, 427 Swanston St. 6 pm

Sydney (www.meetup.com/sydney-2600/): Club York Sydney, 99 York St. 6:30 pm

COLOMBIA

Medellin: El Primer Parque de Laureles. 6 pm

FINLAND

Helsinki: Mall of Tripla food court (2nd floor).

FRANCE

Paris: Place de la République, 1st floor of the Burger King, 10th arrondissement.

IRELAND

Dublin: The Molly Malone Statue on Suffolk St. 7 pm

JAPAN

Tokyo: Beemars, Kabukicho, 2 Chome-27-12 Shinjuku Lee Building #2 3rd floor. 7 pm

KAZAKHSTAN

Almaty: Hoper's Bar, 93a Prospekt Gagarina.

PORTUGAL

Lisbon: Amoreiras Shopping Center, food court next to Portugalia. 7 pm

RUSSIA

Petrozavodsk: Good Place, pr. Pervomayskiy, 2. 7 pm

SPAIN

Madrid (2600.madrid): Maldito Querer, C. de Argumosa, 5. 7 pm

SWEDEN

Malmo (@2600Malmo): FooCafé, Carlsatan 12A.

Stockholm (@2600Stockholm): Urban Deli, Sveavägen 44.

U.K.

England

Bournemouth (@bournemouth2600): The Goat & Tricycle, 27-29 W Hill Rd. 6:30 pm

Cheltenham (@2600Cheltenham): Bottle of Sauce, Ambrose St. 6:30 pm

London (@London_2600): Angel Pub, 61 St Giles High St, outdoors at the red telephone box. 6:30 pm

Manchester (@2600Manchester): Piccadilly Central, 38 London Rd. 6:30 pm

Scotland

Glasgow ([@2600@glasgow.social](http://www.2600glasgow.com)): The Geek Rooms, 151 Bath Ln. 6 pm

URUGUAY

Montevideo: MAM Mercado Agrícola de Montevideo, José L Terra 2220, Choperia Mastra. 7 pm

U.S.A.

Arizona

Phoenix (Tempe) (@PHX2600): Escalante Community Center, 2150 E Orange St. 6 pm

Prescott: Merchant Coffee, 218 N Granite St.

Arkansas

Fort Smith: Fort Smith Coffee Company, 70 S 7th St. 7 pm

California

Fullerton: (www.meetup.com/OC2600/) 23b Shop, 418 E Commonwealth Ave, Unit 1. 7 pm

Los Angeles (www.2600.la/) **@LA2600:** Union Station inside the main entrance by Alameda St near Traxx Bar. 6 pm

Sacramento: Old Soul @ 40 Acres coffee shop, 3434 Broadway. 6 pm

San Francisco: 4 Embarcadero Center, ground level by info kiosk. 6 pm

San Jose: Outside the MLK Library, 6 pm

Colorado

Denver (@denver2600): Denver Pavilions. 6 pm

Fort Collins: Starbucks, 4218 College Ave. 7 pm

Connecticut

Farmington: Barnes & Noble cafe area, 1599 South East Rd.

District of Columbia

Arlington: First floor food court by Sakina's at Fashion Centre at Pentagon City, 1100 S Hayes St.

Florida

Boca Raton: Barnes & Noble on Glades Rd.

Jacksonville (#Jax2600): The Silver Cow, 929 Edgewood Ave S.

Georgia

Atlanta (at12600.org) (@At12600): Lenox Square Mall, 3393 Peachtree Rd NE. 6 pm

Illinois

Oak Lawn ([@OakLawn2600](http://oaklawn2600.com)): The Meta-Center, 4606 W 103rd St, Ste B.

Urbana-Champaign: Harvest Market mezzanine. 6 pm

Indiana

South Bend (sb2600.com): Cloud Walking Cafe.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall. 6 pm

Louisiana

New Orleans: Z'otz Cafe, 8210 Oak St #2042.

Maine

Bangor (Hermon) (@2600Bangor): Bangor Makerspace, 34 Freedom Pkwy

Massachusetts

Boston (Cambridge) (@2600boston): The Garage, Harvard Square, food court area. 7 pm

Hyannis: Nifty Nate's, 246 North St.

Michigan

Lansing: The Fledge, 1300 Eureka St. 6 pm

Minnesota

Bloomington: Mall of America, north food court by Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hackerspace, 2215 Scott Ave.

New Hampshire

Milford (@nh2600@defcon.social): Grill 603, 168 Elm St. 6:30 pm

New Jersey

North Brunswick (@2600NJ): FUBAR Labs, 1510 Jersey Ave.

New York

Albany: UAlbany ETEC Bldg, 1220 Washington Ave. 6 pm

New York ([@NYC2600](http://nyc2600.net)): Citigroup Center, 53rd St & Lexington Ave, food court.

Rochester ([@roc2600](http://rochester2600.com)): Global Cybersecurity Institute, 78 Rochester Institute of Technology. 7 pm

North Carolina

Raleigh (@rtp2600): Transfer Co Food Hall, 500 E Davie St. 7 pm

Ohio

Youngstown: Denny's Restaurant, 4020 Belmont Ave. 6 pm

Oklahoma

Oklahoma City: Big Truck Tacos, 530 NW 23rd St.

Oregon

Portland: Sizzle Pie Central Eastside, 624 E Burnside St. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St.

Lancaster (Columbia) (pa2600.wixsite.com/pa2600): Trio Bar & Grill. 3 pm

Philadelphia (philly2600.net/) (jawns.club/@philly2600): Iffy Books, 404 S 20th St. 6 pm

Tennessee

Memphis (memsec.info): Midsouth Makers, 2804 Bartlett Rd, #3

Texas

Austin (@atx2600): Central Market mezzanine level, 4001 N Lamar Blvd. 7 pm

Dallas: The Wild Turkey, 2470 Walnut Hill Ln #5627.

Houston (www.hou2600.org) **@houston2600:** Agora Coffee House, 1712 Westheimer Rd. 6 pm

San Antonio: PH3AR/Geekdom, 110 E Houston St. 6 pm

Utah

Salt Lake City: 801labs Hackerspace 353 E 200 S, Ste B. 6 pm

Virginia

Arlington: (see District of Columbia)

Hampton: Barnes & Noble cafe, Peninsula Town Center.

Washington

Seattle: Merchant Saloon in Pioneer Square, downstairs. 6 pm

Spokane: Starbucks near Wellesley & Division (across from North Town Mall).

West Virginia

Charleston: KDE Technology, 111 Hale St.

All meetings take place on the first Friday of the month. Unless otherwise noted, 2600 meetings begin at 5 pm local time. Follow @2600Meetings on Twitter and let us know your meeting's Twitter, Mastodon, or Bluesky handle so we can stay in touch and share them here! To start a meeting in your city, DM us or send email to meetings@2600.com.

Earthbound Payphones



Singapore. Yes, you can actually find payphones here, but the odds of them working are slim. This one was spotted east of Grange Road on Tanglin Road.

Photo by Sam Pursglove



Bahamas. Discovered in Rawson Square located in downtown Nassau, we're pretty sure this one isn't working. It makes us wonder how many smashed receivers are the result of the disappointment felt when there's no dial tone.

Photo by Tyson



Brazil. This payphone lives inside of a university in Curitiba (the Universidade Tecnológica Federal do Paraná), which is probably why it's in such good shape. And it still works!

Photo by Eduardo Rhenius



Greece. Our streak continues, as this phone also works! Found at the general hospital of Kavala (fifth floor if you really need to pay it a visit).

Photo by Emmanuel

Visit www.2600.com/payphones to see our foreign payphone photos!
(or turn to the inside front cover to see more right now)

The Back Cover Photos



As if Howe, Texas doesn't already lend itself to all sorts of wordplay, **dale** has discovered their population happens to be a very special number. This is the first city we've ever seen that has exactly the right number of people.



So this starts out good and gets even better. **Warren Smith** found a road that by definition could not be found. It turns out this is the road to Redditt, Ontario (Canada). We couldn't make this up. But we're not done. Until 1985, the main street of Redditt was called Highway 666. And *that* resulted in members of an Evangelical Christian church arguing to the Ministry of Transportation that it was inappropriate for their church to be located on the "highway to Hell." So that road's now known as the far-less-fun Highway 658. But the unfindable 404 Road remains.

If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a 2600 t-shirt of your choice.